RISK MANAGEMENT
PROGETTO S1/L5

Indice

1. Traccia

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 e modellizzazione 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.

2. Risk Scope della TechnoCorp

La TechnoCorp rappresenta ad oggi un'azienda di spicco nel settore della Tecnologia dell'Informazione e dei servizi IT con tre sedi regionali, 500 dipendenti e un bacino di clienti molto ampio che spazia, solo per citarne alcuni, dal settore bancario, a quello medico e assicurativo.

Con oltre 15 anni di esperienza nel fornire consulenza specializzata, sviluppo software su misura e gestione delle infrastrutture tecnologiche, l'azienda si propone di rimanere competitiva, garantire un'elevata qualità dei prodotti di software e di gestire efficacemente le piattaforme digitali di cui si fa carico.

L'azienda ci ha incaricato di svolgere un risk assessment al fine di identificare e valutare la probabilità che un evento avverso possa realizzarsi e determinare l'entità del danno conseguente alla concretizzazione dell'evento stesso.

La TechnoCorp può vantare la gestione di dati e informazioni di clienti particolarmente rilevanti ma anche dati personali dei propri dipendenti.

Questo fa sì che un obiettivo fondamentale per l'azienda sia la protezione e tutela dei dati, informazioni sensibili di clienti, dipendenti e interne.

I dipartimenti aziendali della TechnoCorp che saranno coinvolti nel processo di risk assessment sono, in particolare:

Dipartimento IT: Questo dipartimento è responsabile della gestione e della sicurezza dell'infrastruttura IT, inclusi server, reti, dispositivi, sistemi di sicurezza come firewall perimetrali e software di rilevamento delle minacce. Per tale motivo le attività di tale dipartimento sarebbero direttamente impattate dalla violazione dei dati.

Dipartimento di Sicurezza informatica: Poiché tale reparto dell'azienda si occupa dell'analisi, risposta e gestione degli incidenti e minacce informatiche è direttamente coinvolto nella mitigazione e risposta al rischio della violazione dei dati.

Dipartimento legale: la violazione dei dati pone un problema di violazione di normative come il GDPR, esponendo la società a notevoli conseguenze in termini di sanzioni economiche e di azioni legali da parte degli utenti-vittime.

Dipartimento delle risorse umane: Il dipartimento delle risorse umane potrà essere coinvolto nell'implementazione di politiche di formazione sulla sicurezza informatica per il personale e sulla gestione degli accessi dei dipendenti ai dati sensibili dei clienti.

3. Identificazione di uno scenario di rischio (Top - down)

Questo report presenta un'analisi approfondita del rischio associato alla violazione di dati sensibili in TechnoCorp, che ha implementato al suo interno una politica **Bring You Own Device** (**BYOD).**

Questa politica prevede di consentire ai dipendenti di utilizzare i propri dispositivi personali come smartphone, tablet o laptop per scopi lavorativi.

In un ambiente BYOD quindi i dipendenti utilizzano i loro dispositivi personali per accedere alle risorse aziendali come email, applicazioni, database e altri strumenti di lavoro e si connettono alla rete aziendale. I potenziali vantaggi che offre sono la maggiore flessibilità, produttività dei dipendenti e riduzione dei costi IT. Tuttavia la sua implementazione presenta anche sfide significative in termini di sicurezza dei dati, gestione dei dispositivi e conformità normativa.

Vantaggi BYOD

Flessibilità e mobilità: consentendo ai dipendenti di utilizzare i propri dispositivi personali per scopi aziendali, l'azienda può offrire loro maggiore flessibilità e mobilità nel lavoro. I dipendenti possono accedere ai dati e alle risorse aziendali da qualsiasi luogo e in qualsiasi momento migliorando l'efficienza e la produttività.

Riduzione dei costi: l'azienda può ridurre i costi associati all'acquisto di hardware e software e alla manutenzione di dispositivi aziendali.

Soddisfazione dei dipendenti: molte persone preferiscono utilizzare i propri dispositivi personali poiché sono familiari con il sistema operativo, le applicazioni e le impostazioni personali. In questo modo l'azienda può aumentare la soddisfazione dei dipendenti e migliorare il clima organizzativo.

Aggiornamento tecnologico: i dipendenti tendono ad avere dispositivi personali più recenti e aggiornati rispetto agli hardware aziendali tradizionali. Consentendo loro di utilizzare i propri dispositivi, l'azienda può beneficiare di tecnologie più recenti senza dover investire in costosi aggiornamenti.

***Miglioramento della sicurezza*:** se implementata correttamente, una politica BYOD può migliorare la sicurezza aziendale. L'azienda può imporre misure di sicurezza come l'installazione di software antivirus, l'utilizzo di VPN e il controllo dell'accesso ai dati aziendali, contribuendo a proteggere i dati sensibili e a prevenire violazioni della sicurezza.

***Aumento della flessibilità IT*:** non dovendosi occupare con troppo sforzo della manutenzione hardware/software dei dispositivi, l'azienda può invece concentrarsi maggiormente sulla gestione dei dati e delle applicazioni. Ciò può aumentare la flessibilità e la capacità di adattamento del dipartimento IT alle esigenze aziendali in continua evoluzione.

Problematiche BYOD

***Sicurezza dei dati*:** una delle principali preoccupazioni è la sicurezza dei dati. Utilizzando dispositivi personali c'è il rischio che i dipendenti possano memorizzare o trasferire dati aziendali sensibili su dispositivi non sicuri o compromessi, aumentando il rischio di violazioni della sicurezza dei dati.

***Perdita o furto dei dispositivi*:** i dispositivi personali possono essere soggetti a perdita o furto, mettendo a rischio i dati aziendali memorizzati o accessibili su di essi. Senza misure di sicurezza adeguate ciò potrebbe portare a una compromissione della sicurezza dei dati.

***Controlli di accesso inadeguati*:** i dispositivi personali potrebbero non avere i controlli di accesso adeguati per proteggere l'accesso ai dati aziendali. Questo potrebbe consentire a utenti non autorizzati di accedere alle risorse aziendali o di esporre i dati a rischi di perdita o compromissione.

***Mancanza di controllo sulle applicazioni*:** l'azienda potrebbe avere difficoltà a controllare o limitare le applicazioni installate sui dispositivi personali dei dipendenti. Le applicazioni non autorizzate potrebbero rappresentare rischi per la sicurezza o compromettere le conformità alle normative aziendali.

***Protezione della privacy*:** l'utilizzo di dispositivi personali può sollevare preoccupazioni legate alla privacy dei dipendenti, specialmente se l'azienda implementa misure di monitoraggio o controllo sui dispositivi.

L’obiettivo dell’analisi è quello di identificare i potenziali rischi, valutare gli asset aziendali coinvolti, analizzare le vulnerabilità e le minacce, modellare le minacce, descrivere gli scenari di rischio e condurre un’analisi semi-quantitativa di uno specifico rischio associato.
Il presente report si focalizza sull’ identificazione di uno scenario di rischio collegato ad uno dei principali obiettivi di sicurezza aziendale: la protezione dei dati sensibili, quali informazioni personali, finanziarie o commerciali, brevetti e know-how.

3.1 Analisi degli asset

Al fine della nostra analisi abbiamo bisogno di identificare e valutare gli asset aziendali presenti.

Identificazione degli Asset

RETE AZIENDALE E RETE WIRELESS

Software:

Software di applicazioni aziendali critiche: 9

Si tratta di programmi progettati per la gestione e ottimizzazione di una vasta gamma di operazioni aziendali fondamentali quali contabilità e finanza, gestione delle risorse umane e gestione della supply-chain.

Software di database: 8

Asset intangibile fondamentale perché consente la memorizzazione dei dati in modo strutturato e relazionale permettendo l’efficiente e rapido aggiornamento delle informazioni aziendali. Utilizzando complessi algoritmi e strutture dati ottimizzate, permette di memorizzare, recuperare e aggiornare informazioni in modo rapido ed efficiente, garantendo allo stesso tempo l'integrità e la coerenza dei dati.

Software di archiviazione dati: 7.5

Questo strumento consente di conservare una vasta gamma di dati, sia strutturati che non strutturati, su diversi supporti di memorizzazione. Nel caso della TechnoCorp questo software è ospitato sul server interno.

Sistemi di sicurezza: 7.8

Firewall perimetrale: opera a livello di rete agendo come un filtro tra la Intranet e Internet. Utilizzando regole di sicurezza predefinite, il firewall esamina il traffico di rete in entrata e in uscita per determinare se deve essere consentito o bloccato.
EDR (Endpoint Detection and Response): Tecnologia progettata per rilevare, analizzare e rispondere a minacce informatiche a livello di end point, come server, computer e dispositivi mobili.

Server interni: 10

Dispositivi che agiscono da hub centrale per l'archiviazione, l'elaborazione e la distribuzione dei dati all'interno dell'ambiente IT aziendale. Sono fondamentali per l'azienda perché forniscono risorse computazionali e di archiviazione per supportare una vasta gamma di funzioni, tra cui la gestione dei dati.

Dispositivi di rete per la connettività interna, anche wireless, e l'accesso ai cloud pubblici: 7.5

Router, switch, access point wireless e altri componenti che consentono la connettività all'interno della rete aziendale e l'accesso ai servizi e alle risorse basati sul cloud. I dispositivi di rete sono fondamentali ma sono facilmente sostituibili nonostante siano critici per le operazioni aziendali.

Dispositivi personali e workstation utilizzati dai dipendenti: 9.5

L'azienda ha una politica di bring your own device che consente agli utenti di lavorare con i propri computer accedendo alle risorse aziendali. Per quanto tali beni non rientrino specificamente nella nozione di asset aziendali, sono stati inseriti per la loro

importanza nella gestione del rischio, potendo rappresentare una seria minaccia per la protezione dati.

Licenze dei software: 8.5

Essendo presumibilmente fornitori di software propri ma allo stesso tempo fruitori di software di terze parti, le licenze e la relativa documentazione è fondamentale per la garanzia della conformità legale e la corretta gestione dei diritti di proprietà intellettuale.

SERVIZI DIGITALI

Applicazioni e servizi utilizzati su cloud pubblici (AWS, Azure): 8

L'azienda si avvale di servizi di cloud pubblici, cioè di risorse e applicazioni che sono fornite dal provider cloud anziché gestire tali risorse sul proprio ambiente IT interno. La presenza di dati e informazioni sensibili li rende di medio/alta rilevanza nel risk assessment in esame, poiché un attacco di hacking potrebbe portare alla perdita, manomissione o indisponibilità dei dati.

Sito web ospitato esternamente: 7

L'azienda utilizza servizi di hosting web forniti da terze parti per rendere accessibile il proprio sito web su internet.

Dati sensibili e informazioni aziendali, inclusi dati finanziari, personali e proprietà intellettuale: 10

Si tratta di una delle risorse aziendali di maggior rilevanza perché, se divulgati, resi accessibili o utilizzati in modo improprio mettono a rischio la protezione della privacy e comportano danni reputazionali e finanziari rilevanti.

RISORSE UMANE

Dipendenti aventi accesso ai dati sensibili e alle applicazioni aziendali: 9

Si tratta di un “asset” che può esporre facilmente i dati al rischio di attacchi informatici perché sono il bersaglio privilegiato dai black hat, anche in considerazione del fatto che potrebbero usare dispositivi personali infetti o in generale compromessi per il loro lavoro.

- *Amministratori di sistema con accesso totale all’infrastruttura: 8*
- *Sviluppatori con accesso ai sistemi di sviluppo:7.5*
- *Personale di supporto tecnico con accesso limitato: 6*

Consulenti e collaboratori esterni con credenziali di accesso: 7.5

Valutazione degli Asset

L’ identificazione dei beni aziendali consente di valutare la loro importanza strategica (nella tabella “IS”) e capire quanto possano essere impattati dal rischio di attacchi informatici. Si procederà alla descrizione degli asset con relativa assegnazione di un punteggio, da 0 (minima rilevanza) a 10 (massima rilevanza) per la loro classificazione in base al rischio associato.

ASSET	IS	Quantità	Costo Asset	Valore Asset
Software	**8**	3	200.000 €	È elevato considerando licenze, manutenzione, dati sensibili, integrazione con l'infrastruttura IT aziendale (come reti, server e sistemi di archiviazione), obsolescenza tecnologica.
Server	**10**	30	90.000 €	Dobbiamo considerare i costi di gestione, di manutenzione, costi energetici, licenze, obsolescenza tecnologica.
Dipendenti	**8.5**	400	1.000.000 €/mese	Dobbiamo considerare la formazione e il costo delle certificazioni necessarie.
Dispositivi di rete	**7.5**	7	14.000 €	Consideriamo manutenzione, gestione, durata e ammortamento e il loro impatto sulle operazioni aziendali

Dispositivi personali	**9.5**	400	————	È critico per la possibilità di veicolare malware e compromettere l'intera rete aziendale ma anche per la possibilità di furto di dati sensibili.
Dati	**10**	5 terabyte	————	Maggior rilevanza perchè, se divulgati, resi accessibili o utilizzati in modo improprio mettono a rischio la protezione della privacy e comportano danni reputazionali e finanziari rilevanti.
Cloud pubblici	**8**	(AWS, Azure)	30.000 €	La presenza di dati e informazioni sensibili li rende di medio/alta rilevanza, anche perché un attacco di hacking potrebbe portare alla perdita, manomissione o indisponibilità dei dati.
Sito web esterno	**7**	1	————	Fatturato 10.000 €/giorno. Più elevato considerando l'impatto sulla reputazione aziendale e la perdita finanziaria in caso di interruzione del servizio.
Sistemi di sicurezza	**7.8**	Firewall, IDS e SIEM	25.000 €	Hanno funzioni principali come la protezione dei dati aziendali, delle infrastrutture IT, delle risorse fisiche, la gestione del rischio ed il miglioramento della reputazione.

Per fornire un valore monetario ipotetico dell'infrastruttura IT di TechnoCorp possiamo considerare un valore complessivo basato su una stima delle attrezzature e delle risorse necessarie per supportare le operazioni aziendali. Supponiamo che l'azienda abbia investito in un'infrastruttura IT robusta e diversificata per supportare le sue attività di consulenza, sviluppo software e gestione delle infrastrutture tecnologiche. Consideriamo un ampio spettro di risorse che includono server fisici, servizi cloud, reti e altre risorse informatiche. Potremmo stimare il valore complessivo dell'infrastruttura IT dell'azienda nell'intervallo di diversi milioni di euro, ad esempio tra 3 e 5 milioni. Nel nostro caso prenderemo in considerazione la media dell'intervallo

sopra indicato, quindi stimiamo il valore di questo insieme di asset per un totale di **4 milioni di €**.
È importante considerare anche l'impatto sulla **reputazione aziendale.**

3.2 Analisi delle vulnerabilità

L'analisi della vulnerabilità è un 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 quelle fisiche, tecniche e operative proprie dell'asset.

Nel contesto BYOD in TechnoCorp ci sono diverse vulnerabilità da considerare:

- **Dispositivi non sicuri.** I dipendenti potrebbero utilizzare dispositivi personali non adeguatamente protetti, senza criteri di sicurezza appropriati come password complesse, cifratura dei dati o software antivirus aggiornati. Questo espone l'azienda a rischi di compromissione dati.
- **Errata configurazione di software/hardware.** Se i dispositivi personali non sono correttamente gestiti o configurati esiste il rischio che persone non autorizzate possano accedere alle risorse aziendali come email, documenti sensibili o applicazioni aziendali.
- **Manutenzione e aggiornamenti insufficienti.** I dipendenti potrebbero non mantenere i propri dispositivi aggiornati con le ultime patch di sicurezza e aggiornamenti del software, lasciando le porte aperte per potenziali vulnerabilità.
- **Applicazioni non sicure.** I dipendenti potrebbero installare applicazioni non sicure o non autorizzate sui propri dispositivi, aumentando il rischio di malware o accesso non autorizzato ai dati aziendali.
- **Interconnessione con reti non sicure.** I dipendenti potrebbero utilizzare i propri dispositivi per accedere alla rete aziendale da luoghi pubblici o reti Wi-Fi

non sicure, esponendo i dati aziendali a potenziali attacchi di tipo man-in-the-middle o altri rischi di sicurezza.

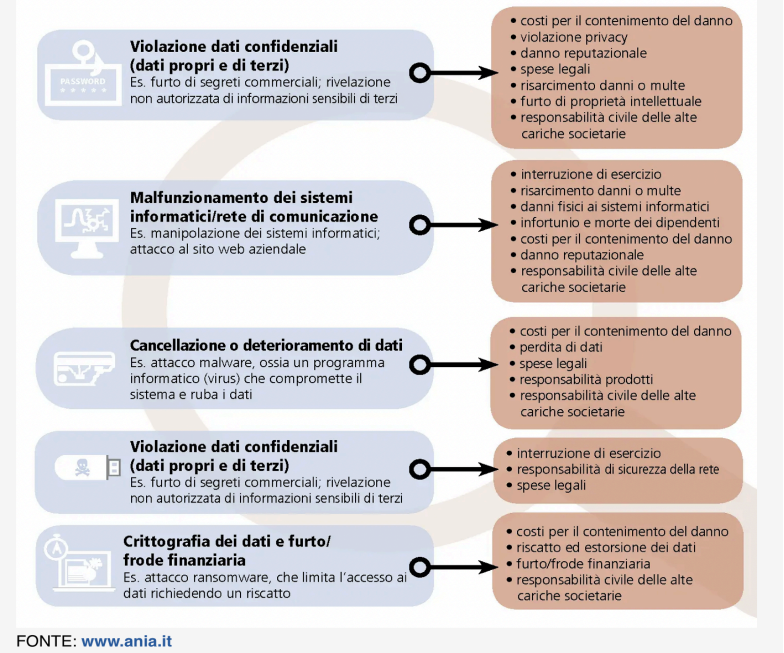
- **Mancanza di controllo IT.** L'azienda potrebbe avere difficoltà nel monitorare e applicare politiche di sicurezza sui dispositivi personali dei dipendenti, soprattutto se non stati implementati adeguati strumenti di gestione della mobilità aziendale (Mobile Device Management - **MDM**).

3.3 Analisi delle minacce

Attraverso una ricerca mirata delle fonti abbiamo ottenuto informazioni utili per condurre l'analisi delle minacce.

Classifica		Percentuale	2022 classifica	Tendenza
1	Rischi informatici *(crimine informatico, malware/ransomware, violazione dei dati, guasti IT)*[1]	34%	*1 (44%)*	→
2	Interruzione di attività *(anche della supply chain)*	34%	*2 (42%)*	→
3	Cambiamenti nello scenario macro economico *(programmi di « austerity », aumento del prezzo dei beni di consumo primari, inflazione/deflazione)*	25%	*10 (11%)*	↑
4	Crisi energetica *(carenza/interruzione della fornitura, fluttuazioni dei prezzi)*	22%	NUOVO	↑
5	Cambiamenti nello scenario legislativo e regolamentare *(sanzioni economiche, protezionismo, disgregazione dell'Eurozona)*[2]	19%	*5 (19%)*	→
6	Catastrofi naturali *(tempeste, inondazioni, terremoti)*	19%	*3 (25%)*	↓
7	Cambiamento climatico *(rischi fisici, operativi, finanziari e di reputazione derivanti dal riscaldamento mondiale)*	17%	*6 (17%)*	↓
8	Carenza di manodopera qualificata[3]	14%	*9 (13%)*	↑
9	Incendio, esplosioni	14%	*7 (17%)*	↓
10	Rischi politici *(guerra, terrorismo, sommosse)*	13%	*13 (9%)*	↑

Associamo quindi le minacce più comuni alle loro possibili conseguenze.



FONTE: www.ania.it

Minaccia	Descrizione	Vettore di attacco	Fonte di minaccia	Probabilità (prima)	Controllo di mitigazione	Probabilità (dopo)
Malware Ransomware	Cripta i dati dell'organizzazione con richiesta di riscatto	Email di phishing, siti web malevoli	Attori criminali	ALTA	Formazione sulla sicurezza informatica, software antivirus/antimalware, backup regolari	BASSA
BYOD	Intrusioni veicolate dai dispositivi personali	Dispositivi BYOD	Hacker, Insider	ALTA	Controllo rigido sugli accessi	MEDIA
Furto di dispositivi	Furto o esposizione dei dispositivi personali	Dispositivi portatili persi	Ladri	MEDIA	———	———
Accesso non autorizzato	Hacking dei sistemi tramite sfruttamento di vulnerabilità	Rete, applicazioni web	Hacker, Insider	MEDIA	Autenticazione a due fattori (2FA), VPN, segmentazione della rete	BASSA
Perdita di dati	Furto o esposizione di dati sensibili	Insider, data breach	Insider, Hacker	BASSA	Crittografia dei dati, DLP (Data Loss Prevention), controllo degli accessi	MOLTO BASSA
Errore Umano	Configurazioni errate, violazioni di policy di sicurezza	Azioni degli utenti interni	Dipendenti	ALTA	Formazione sulla sicurezza informatica, policy di sicurezza chiare e definite	MEDIA

3.4 Modellizzazione delle minacce

Una minaccia è una potenziale causa di un incidente indesiderato che può produrre danni a un sistema o a un'organizzazione.

L'analisi delle minacce (threat analysis) è un processo sistematico che mira a identificare tutte le minacce che hanno una ragionevole probabilità di verificarsi e quindi possono compromettere la sicurezza di un'organizzazione, di un sistema o di un asset.

Le principali attività dell'analisi delle minacce sono:

- **Identificazione:** individuare ed elencare tutte le possibili minacce che potrebbero sfruttare le vulnerabilità dell'organizzazione o del sistema preso in esame.
- **Caratterizzazione:** raccogliere informazioni dettagliate su ciascuna minaccia, come la sua natura, le modalità di attacco, le potenziali conseguenze e l'eventuale attore che potrebbe metterla in atto.
- **Valutazione:** analizzare e valutare le minacce identificate in termini di probabilità di occorrenza e impatto potenziale.

L'identificazione consiste nel riconoscere tutte le potenziali minacce che potrebbero colpire i beni, le risorse o i processi dell'organizzazione in esame.

In questa prima fase si cerca già di discriminare tra minacce che potrebbero verificarsi o no. In condizioni di dubbio si procede comunque all'inserimento della minaccia in elenco in attesa di approfondimenti nelle fasi successive.

L'identificazione può avvenire da diverse fonti, tra cui la modellizzazione delle minacce (**threat modeling**).

Il threat modeling è il 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.

Un **threat model** è una rappresentazione strutturata di tutte le informazioni che influiscono sulla sicurezza di un asset.

Il threat model che riteniamo essere più adatto al nostro caso è quello delle **quattro domande di Adam Shostack.**

Questa modellizzazione prevede di porsi quattro domande chiave per identificare le minacce:

1. Su cosa stiamo lavorando?
2. Cosa può andare storto?
3. Cosa possiamo fare a riguardo?
4. Abbiamo fatto un buon lavoro?

1) Su cosa stiamo lavorando?

TechnoCorp prevede come ramo operativo aziendale la gestione di dati sensibili. L'obiettivo del nostro lavoro verte sulla protezione di questi dati nel contesto BYOD.

2) Cosa può andare storto?

Nel contesto BYOD in TechnoCorp troviamo una vasta gamma di minacce:

- **Perdita o furto di dispositivi.** Se un dispositivo personale di un dipendente viene perso o rubato, i dati aziendali sensibili potrebbero essere compromessi. Ciò potrebbe includere dati dei clienti, segreti aziendali o proprietà intellettuale.
- **Malware e virus.** I dispositivi BYOD potrebbero essere più vulnerabili a malware e virus rispetto ai dispositivi aziendali gestiti. Ciò è dovuto dal fatto che

i dispositivi personali dei dipendenti potrebbero non avere le stesse misure di sicurezza in atto e potrebbero essere utilizzati per accedere a reti non sicure.

- **Phishing e attacchi di ingegneria sociale.** I dipendenti che utilizzano dispositivi BYOD potrebbero essere più suscettibili a phishing e attacchi di social engineering. Ciò è dovuto al fatto che potrebbero essere meno attenti quando utilizzano dispositivi personali e potrebbero essere più propensi a fare clic su collegamenti o aprire allegati dannosi.
- **Attacchi ransomware.** Le conseguenze dell'infezione da ransomware possono essere devastanti per le vittime, con la perdita di dati importanti, interruzioni delle operazioni aziendali e potenziali costi finanziari significativi dovuti al pagamento del riscatto o alla riparazione dei danni causati dall'attacco.

3) Cosa faremo a riguardo?

Per affrontare le minacce nel contesto BYOD descritto nel caso di TechnoCorp è fondamentale implementare una serie di azioni di mitigazione per proteggere i dati aziendali sensibili e ridurre il rischio di compromissione.

- **Politiche di sicurezza.** Stabilire politiche BYOD robuste e ben comunicate che delineino i requisiti di sicurezza per i dispositivi personali utilizzati dai dipendenti.
  Queste politiche dovrebbero includere requisiti di sistemi di sicurezza per la protezione dei dispositivi come la crittografia dei dati, l'uso di password complesse, l'attivazione del software antivirus e la configurazione dei dispositivi in conformità con gli standard aziendali.
- **Soluzioni di gestione dei dispositivi mobili (MDM).** Implementare una soluzione MDM (Mobile Device Management) per consentire alle aziende di gestire e controllare in modo centralizzato i dispositivi BYOD.
  Con un MDM è possibile applicare politiche di sicurezza coerenti su tutti i

dispositivi come il blocco remoto dei dispositivi smarriti o rubati, la cancellazione dei dati da remoto o la distribuzione di patch e aggiornamenti critici del software.

- **Formazione sulla sicurezza e consapevolezza dei dipendenti.**
  Condurre sessioni di formazione regolare per educare i dipendenti sulle minacce alla sicurezza informatica, compresi i rischi specifici associati all'uso dei dispositivi BYOD.
  Insegnare ai dipendenti come riconoscere ed evitare phishing, attacchi di social engineering e comportamenti online rischiosi che potrebbero mettere a rischio la sicurezza dei dati aziendali.
- **Monitoraggio e rilevamento delle minacce.** Implementare strumenti e soluzioni per il monitoraggio e il rilevamento delle minacce sui dispositivi BYOD e nelle reti aziendali.
  Utilizzare sistemi di sicurezza avanzati per identificare e rispondere rapidamente a comportamenti sospetti o anomalie che potrebbero indicare un attacco malware, phishing o ransomware.
- **Backup regolari.** Implementare un piano di backup regolare dei dati critici per mitigare il rischio di perdita dei dati dovuta ad attacchi ransomware o altre minacce informatiche. Assicurarsi che i processi di backup e ripristino dati siano testati e documentati.
- **Controllo degli accessi.** Implementare controlli e sistemi di monitoraggio degli accessi adeguati e robusti per proteggere l'accesso ai dati sensibili.

4) Abbiamo fatto un buon lavoro?

Per valutare se le implementazioni delle azioni di rimedio sopra citate sono efficaci e se hanno contribuito a mitigare le minacce identificate possiamo utilizzare una serie di misure e metriche di valutazione.

- **Conformità alle politiche di sicurezza.** Verificare se i dipendenti rispettano e seguono le politiche di sicurezza BYOD stabilite tramite l'uso di strumenti di controllo e reportistica.
- **Tassi di incidenti di sicurezza.** Analizzare i tassi di incidenti di sicurezza relativi ai dispositivi BYOD prima e dopo l'implementazione delle azioni di mitigazione. Un calo significativo negli incidenti di sicurezza potrebbe indicare un miglioramento della sicurezza complessiva.
- **Feedback e coinvolgimento dei dipendenti.** Il coinvolgimento attivo dei dipendenti nel processo di sicurezza può fornire informazioni prezione sulla percezione dell'efficacia delle politiche e delle procedure.
- **Test di penetrazione e valutazioni della sicurezza.** Condurre test di penetrazione e valutazioni della sicurezza periodiche per identificare eventuali nuova vulnerabilità o debolezze nel sistema. Monitorare i risultati di questi test per assicurarsi che le misure di sicurezza siano ancora efficaci nel tempo.
- **Conformità normativa.** Assicurarsi che le azioni di mitigazione implementate siano conformi alle normative e ai requisiti di sicurezza applicabili. Monitorare la conformità continua e adattare le misure di sicurezza di conseguenza.
- **Riduzione dei rischio.** Monitorare il cambiamento nel rischio attraverso l'analisi delle probabilità e degli impatti delle minacce e valutare se le misure di mitigazione abbiano ridotto efficacemente questo rischio.
- **Risultati finanziari.** Esaminare l'impatto finanziario delle azioni di mitigazione implementate. Ad esempio valutare i costi associati agli incidenti di sicurezza prima e dopo l'implementazione delle misure di sicurezza per determinare eventuali risparmi o perdite finanziarie.

3.5 Scenari di rischio

Dopo aver analizzato le fonti online, il NIST e le normative ISO abbiamo identificato più scenari di rischio che valuteremo utilizzando la loro frequenza ed entità.
Ecco quattro scenari di rischio associati alla politica Bring Your Own Device (BYOD):

1. Perdita o Furto del Dispositivo:
    - **Probabilità di Occorrenza:** Alta
    - **Livello di Impatto:** Alto
    - **Rischio:** Alto
    - **Descrizione:** I dispositivi personali utilizzati per scopi lavorativi possono essere persi o rubati, esponendo dati sensibili.
2. Malware e Ransomware:
    - **Probabilità di Occorrenza:** Medio
    - **Livello di Impatto:** Alto
    - **Rischio:** Alto
    - **Descrizione:** L'installazione di app non verificate può introdurre malware che compromette la sicurezza dei dati aziendali.
3. Accesso Non Autorizzato:
    - **Probabilità di Occorrenza:** Medio
    - **Livello di Impatto:** Medio
    - **Rischio:** Medio
    - **Descrizione:** La mancanza di misure di sicurezza adeguate può permettere l'accesso non autorizzato ai dati aziendali.
4. Conflitto tra Applicazioni e Dati Aziendali:
    - **Probabilità di Occorrenza:** Medio
    - **Livello di Impatto:** Basso
    - **Rischio:** Basso

- **Descrizione:** Le applicazioni personali possono interferire con le applicazioni e i dati aziendali, portando a problemi di compatibilità e potenziale perdita dei dati

Lo scenario preso in considerazione per l'analisi semi-quantitativa è quello relativo ai Ransomware.

4. Analisi del rischio semi-quantitativa

L'analisi del rischio è un'indagine dettagliata volta a comprendere la probabilità e l'impatto di un rischio, nonché a sviluppare misure per ridurne la probabilità o l'effetto negativo. L'analisi condotta fino ad ora tiene conto di un insieme di fattori coinvolti che sono interdipendenti e si influenzano reciprocamente: Minacce, Contesto, Asset, Vulnerabilità, Valore degli asset, Tolleranza, Impatto, Mitigazione ed è utile per sviluppare l'analisi del rischio sullo scenario specifico scelto. Abbiamo quindi potuto delineare una visione il più ampia e completa possibile (Top-down) degli scenari presenti per poi diventare sempre più specifica ed operativa in questa sezione.

L'analisi del rischio semi-quantitativa è un metodo per valutare i rischi che combina elementi qualitativi e quantitativi.

Al fine della nostra analisi abbiamo bisogno di alcuni dati come:

- L'**AV** (Asset Value)
  Stima economica dei beni coinvolti nell'analisi del rischio.
  Secondo le nostre stime l'infrastruttura IT di TechnoCorp è pari a
  4.000.000€.

- Il **fatturato annuo**
  Somma dei ricavi totali conseguiti dall'impresa in un determinato anno solare.
  Da calcoli effettuati grazie a dati presi da un report di Assintel (Associazione

Nazionale Imprese ICT) stimiamo un fatturato annuo di circa **200.000.000€**.

- L'**EF** (Exposure Factor)
  Indice che serve a misurare il livello di danno o l'impatto provocato da un evento dannoso su un singolo asset. Viene espresso sotto forma di percentuale compresa tra 0% o 100% del valore dell'asset colpito dalla minaccia.
  Ipotizzando che al verificarsi di una minaccia l'esposizione dei dati sia pari al 100%, il nostro **EF sarà pari a 1**.

- L'**SLE** (Single Loss Expectancy)
  Misura il costo associato ad una singola minaccia che agisce su un singolo asset. Questo valore si calcola moltiplicando il valore degli asset coinvolti (AV) per il fattore di esposizione (EF).
  Quindi:
  SLE = AV * EF = 4.000.000 * 1 = 4.000.000€

- L'**ARO** (Annualized Rate of Occurrence)
  Tasso del numero di volte che una minaccia si verifica nell'arco di un anno. Secondo fonti terze un'azienda della grandezza di TechnoCorp si aspetta attacchi di tipo ransomware due volte l'anno in media.
  ARO = Numero Attacchi / Anni = 2 / 1 = 2

- L'**ALE** (Annualized Loss Expectancy)
  La perdita attesa (potenziale), su base annua, associata ad una specifica minaccia.
  Questo valore lo calcoliamo moltiplicando l'SLE per l'ARO:
  ALE = SLE * ARO = 4.000.000 * 2 = 8.000.000€

- L'**impatto**

  L'impatto è la gravità potenziale del danno causato da un evento pericoloso.

  Lo si calcola dividendo l'ALE per il fatturato annuo:

  I = ALE / Fatturato Annuo = 8.000.000 / 200.000.000 = 0,04 = 4%

- La **verosomiglianza**

  Rappresenta la probabilità che si verifichi un evento pericoloso specifico.

  Secondo le fonti consultate la verosomiglianza di un attacco ransomware è alta ed in continua crescita, stimata in questo caso **pari al 75%**.

STIMA DELLA VEROSOMIGLIANZA

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.

STIMA DELL'IMPATTO

Secondo la tabella H-3 del NIST SP 800-30 Rev. 1 il valore qualitativo dell'impatto corrispondente a quello semi-quantitativo (individuato in precedenza, al 4%) ci permette di classificarlo **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.

STIMA DEL RISCHIO

Combinando le valutazioni quantitative e semi-quantitative della verosomiglianza e dell'impatto siamo in grado di classificare il nostro rischio come low (in accordo con la tabella I-2 del NIST SP 800-30 Rev. 1).

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