EPICODE

S1 - L5

Identificazione e analisi del rischio

29 aprile 2024

Team:

- Alessio D'Ottavio
- Davide Di Turo
- Giuseppe Pigniatello
- Luca Iannone
- Manuel Di Gangi
- Marco Fasani
- Oliviero Camarota

INDICE

Traccia

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

Nome azienda: TechnoCorp

Settore: Tecnologia dell'informazione e servizi IT

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

Infrastruttura IT:

- Rete aziendale con server interni che ospitano applicazioni aziendali critiche, database e sistemi di archiviazione dati
- Utilizzo di cloud pubblici (AWS, Azure) per alcune applicazioni e servizi
- Rete wireless per dipendenti e guest
- Dispositivi personali (Bring Your Own Device) utilizzati dai dipendenti
- Numerosi laptop e workstation per sviluppatori e consulenti
- Sito web aziendale ospitato esternamente
- Firewall perimetrale
- EDR/xDR su tutti i sistemi

Clienti e dati sensibili:

- TechnoCorp gestisce dati sensibili di clienti, come informazioni finanziarie, dati personali di dipendenti/clienti, proprietà intellettuale
- I principali clienti includono banche, assicurazioni, aziende sanitarie e produttori

Personale e accessi:

- Amministratori di sistema con accesso totale all'infrastruttura

- Sviluppatori con accesso ai sistemi di sviluppo
- Personale di supporto tecnico con accesso limitato
- Consulenti e collaboratori esterni con credenziali di accesso
- Politica di password e autenticazione a due fattori implementata

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

- Identificazione del rischio
    - Analisi degli asset
    - Analisi delle vulnerabilità
    - Analisi delle minacce
    - Modellazione delle minacce
    - Scenari di rischio
- Analisi del rischio qualitativa o semi-quantitativa

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

1. Analisi degli asset

1.1 Identificazione degli asset:

Categoria di Asset	Tipo di Asset	Quantità
Server di file	Fisico	6
Server di database	Fisico	15
Server di applicazioni	Fisico	10
Server di posta elettronica	Fisico	2
Server web	Fisico	2
Server di backup e ripristino	Fisico	24
Istanze di server virtuale (VM)	Fisico	60
Servizi di archiviazione dati	Intangibile	100 TB
Servizi di sicurezza cloud	Intangibile	2
Smartphone BYOD	Fisico	300
Tablet BYOD	Fisico	50
Laptop BYOD	Fisico	100
Dispositivi di archiviazione esterna	Fisico	300
Dispositivi IoT	Fisico	30

Laptop aziendale	Fisico	450
Monitor	Fisico	750
Tastiere e mouse	Fisico	750
Periferiche di input/output	Fisico	100
Dispositivi hardware firewall	Fisico	1
Soluzioni software firewall	Intangibile	500
Servizi di firewall gestiti	Intangibile	ND
Software EDR/xDR	Intangibile	500 installazioni
Licenze software EDR/xDR	Intangibile	500 licenze
Console di gestione e monitoraggio EDR/xDR	Fisico	3
Router e switch di rete	Fisico	20
Access point wireless	Fisico	48

1.2 Valutazione dell'importanza:

Per una valutazione completa degli asset di TechnoCorp, utilizzeremo un approccio strutturato che considera l'importanza, l'impatto di una compromissione e un punteggio numerico per facilitare la priorizzazione delle risorse da proteggere. Ecco una valutazione dettagliata con punteggi che riflettono il livello di rischio e la criticità di ogni asset.

1.3 Metodologia di Valutazione

- **Importanza**: Basata sulla necessità operativa dell'asset per l'azienda.
- **Impatto di Compromissione**: Valutato in termini di conseguenze finanziarie, operative e di immagine per l'azienda.
- **Punteggio**: Scala da 1 a 10, dove 10 indica l'importanza massima e l'impatto massimo di una compromissione.

Analisi dettagliata:

Server Interni

- **Importanza**: Critica per l'archiviazione di dati sensibili e la gestione delle operazioni centrali.
- **Impatto di Compromissione**: La perdita o il danneggiamento di questi server causerebbe gravi interruzioni operative e potenziali perdite di dati.
- **Punteggio**: 10, priorità massima di protezione.

Infrastruttura Cloud

- **Importanza**: Alta per scalabilità e accessibilità dei servizi.
- **Impatto di Compromissione**: Interruzioni dei servizi e potenziali violazioni di dati.
- **Punteggio**: 9, richiede elevate misure di sicurezza e monitoraggio costante.

Dispositivi BYOD

- **Importanza**: Supportano la mobilità e la flessibilità del lavoro, ma aumentano l'esposizione a rischi di sicurezza.
- **Impatto di Compromissione**: Alto per il potenziale accesso non autorizzato ai dati aziendali.
- **Punteggio**: 8, necessitano di politiche di sicurezza stringenti e formazione degli utenti.

Laptop e Workstation

- **Importanza**: Essenziali per le operazioni quotidiane dei dipendenti.
- **Impatto di Compromissione**: Interruzione delle attività lavorative e perdita di dati.
- **Punteggio**: 10, protezione critica necessaria per garantire la continuità operativa.

Firewall Perimetrale

- **Importanza**: Critica come prima linea di difesa contro minacce esterne.
- **Impatto di Compromissione**: Compromissione potrebbe esporre l'intera rete aziendale a rischi elevati.
- **Punteggio**: 10, investimenti prioritari in tecnologie avanzate e revisioni di sicurezza frequenti.

EDR/xDR sui Sistemi

- **Importanza**: Alta per la capacità di rilevare e rispondere a minacce in tempo reale.
- **Impatto di Compromissione**: Rischio di non rilevare attacchi in tempo, con conseguenti danni significativi.
- **Punteggio**: 9, fondamentale mantenere aggiornate e operative tutte le soluzioni di sicurezza.

Altri Asset di Rete (Router, Switch)

- **Importanza**: Alta per la gestione del traffico di rete e la connettività.
- **Impatto di Compromissione**: Interruzione della connettività e potenziale accesso non autorizzato.
- **Punteggio**: 9, richiedono una gestione attenta e aggiornamenti regolari.

Categoria di Asset	Importanza	Impatto di Compromissione	Punteggio
Server Interni	Alta	Molto alto	10
Infrastruttura Cloud	Alta	Alto	9
Dispositivi BYOD	Media	Alto	8
Laptop e Workstation	Alta	Molto alto	10
Firewall Perimetrale	Critica	Estremamente alto	10
EDR/xDR sui Sistemi	Alta	Molto alto	9
Altri Asset di Rete (Router, Switch)	Alta	Alto	9

1.3 Determinazione dei costi

Categoria di Asset	Quantità	Costo di Acquisizione (€)	Costo di Manutenzione Annuale (€)	Ammortamento (anni)	Obsolescenza
Server Interni	59	472000	47000	5	5-7 anni
Infrastruttura Cloud	Varie	5000 /mese	0	3	3-5 anni
Dispositivi BYOD	780	390000	78000	2	2-3 anni
Laptop e	2050	1025000	205000	3	3-4 anni

Workstation					
Firewall Perimetrale	5	200000	40000	5	5-7 anni
EDR/xDR sui Sistemi	1003	501500	100300	3	3-5 anni
Altri Asset di Rete (Router Switch)	68	340000	34000	5	5-7 anni

1.4 Spiegazioni e Assunzioni

- Costo di Acquisizione: Stima del costo totale per acquistare l'asset, inclusi hardware e software.
- Costo di Manutenzione Annuale: Include il costo delle operazioni di manutenzione regolare, aggiornamenti, e supporto tecnico.
- Ammortamento: Numero di anni durante i quali l'asset viene ammortizzato contabilmente.
- Obsolescenza: Periodo stimato dopo il quale l'asset diventa obsoleto o richiede un sostituto a causa di avanzamenti tecnologici o usura fisica.

1.5 Note

- I valori sono ipotetici e servono come esempio. Nella realtà, questi costi possono variare in base a negoziazioni con fornitori, specifiche tecniche degli asset, politiche aziendali e dinamiche di mercato.
- Per dispositivi come i BYOD, l'ammortamento e l'obsolescenza sono considerati su una scala temporale più breve a causa della rapida evoluzione della tecnologia mobile.

- Gli asset cloud hanno costi di manutenzione annuali relativamente alti a causa della necessità di aggiornamenti costanti e della gestione della sicurezza in ambienti condivisi.

1.6 Attribuzione del valore

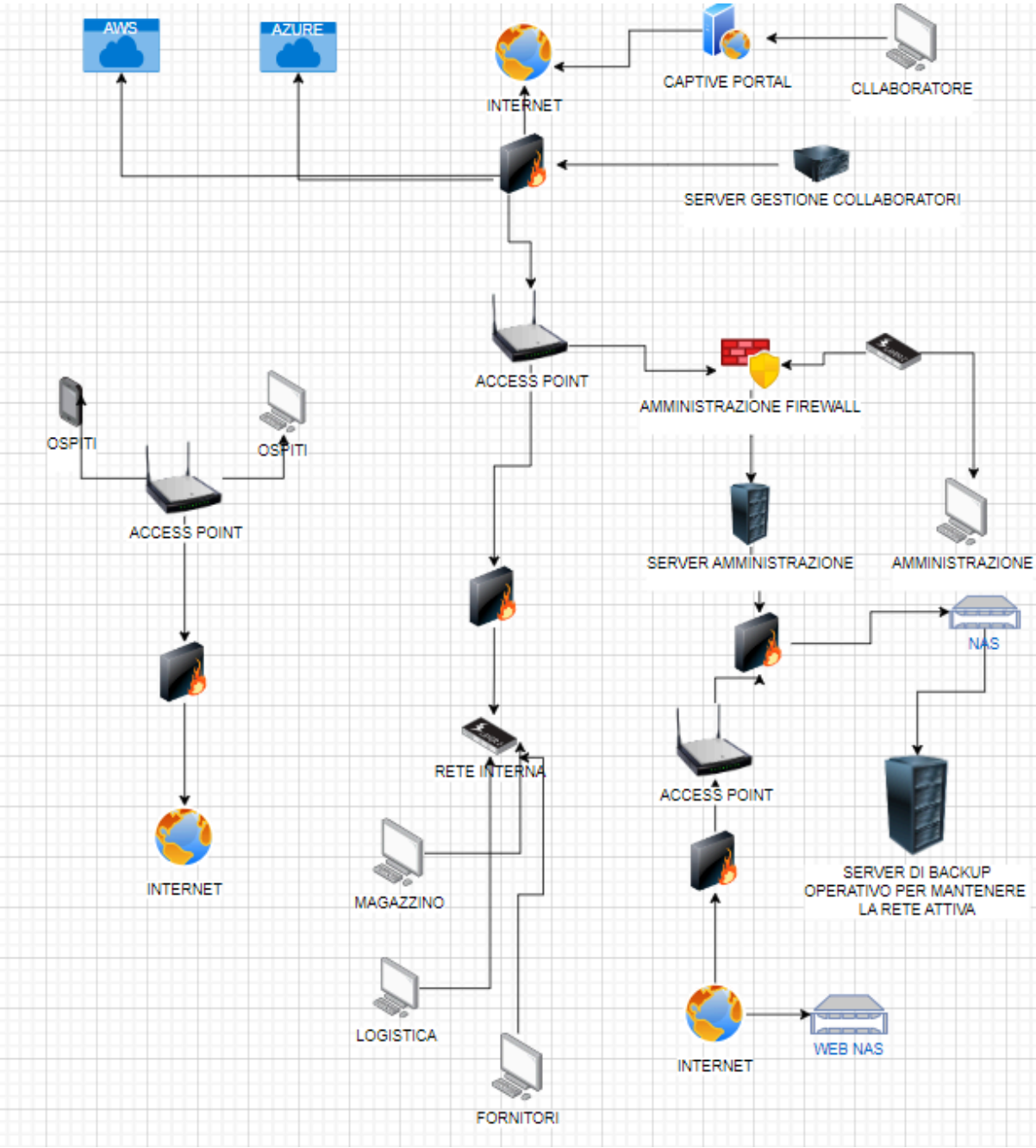
Per realizzare un'attribuzione del valore degli asset di TechnoCorp, considereremo vari elementi come il costo storico, il valore netto attuale, il valore di mercato, il metodo di valutazione utilizzato e note rilevanti sulla valutazione di ciascun asset. Assumeremo che il costo storico sia il costo iniziale di acquisizione e che l'ammortamento sia lineare, con una completa obsolescenza degli asset tecnologici dopo il periodo di ammortamento specificato.

Categoria di Asset	Costo Storico (€)	Valore Netto Attuale (€)	Valore di Mercato (€)	Metodo di Valutazione	Note sulla Valutazione
Server Interni	472000	0	800000	Ammortamento lineare	Completamente ammortizzati, valore residuo stimato dal mercato
Infrastruttura Cloud	5000	5000	0	Ammortamento lineare	Parzialmente ammortizzati, alta domanda di mercato
Dispositivi BYOD	390000	0	50000	Ammortamento lineare	Completamente ammortizzati, basso valore di rivendita
Laptop e Workstation	1025000	341667	500000	Ammortamento lineare	Valore ridotto a causa dell'uso e dell'avanzamento tecnologico
Firewall Perimetrale	200000	0	30000	Ammortamento lineare	Obsolescenza tecnologica, valore residuo basso
EDR/xDR sui Sistemi	501500	167167	250000	Ammortamento lineare	Buon mercato secondario per software di sicurezza aggiornato
Altri Asset di Rete (Router, Switch)	340000	0	70000	Ammortamento lineare	Completamente ammortizzati, valore residuo da vendita di usato

1.6 Metodologia di Valutazione e Note

- **Costo Storico**: Costo originale di acquisizione degli asset.
- **Valore Netto Attuale:** Calcolato sottraendo l'ammortamento accumulato al costo storico. Gli asset completamente ammortizzati hanno un valore netto attuale di zero.
- **Valore di Mercato**: Valore stimato se gli asset fossero venduti nel mercato attuale. Determinato in base alla domanda di mercato, condizioni dell'asset, e obsolescenza tecnologica.
- **Metodo di Valutazione**: L'ammortamento lineare è stato utilizzato per tutti gli asset, assumendo una riduzione costante del valore nel tempo fino a raggiungere l'obsolescenza.
- **Note sulla Valutazione**: Le note forniscono dettagli sulle condizioni del mercato, la domanda e altri fattori che influenzano il valore di mercato degli asset.

1.7 Infrastruttura IT - TechnoCorp



lo schema di rete proposto da noi per efficientare la sicurezza di rete

2. Analisi dell vulnerabilità

2.1. Vulnerabilità legate alla gestione dei privilegi:

Privilegi di accesso non adeguatamente limitati: Gli amministratori di sistema e altri utenti con accesso privilegiato potrebbero avere più accesso di quanto necessario per svolgere le proprie mansioni, aumentando il rischio di abusi o compromissioni dei dati sensibili.

Mancanza di monitoraggio degli accessi privilegiati: Potrebbe mancare un adeguato monitoraggio delle attività degli amministratori di sistema e degli altri utenti con accesso elevato, consentendo loro di agire senza essere rilevati.

2.2. Vulnerabilità legate alla sicurezza dei dispositivi:

Server interni: I server interni potrebbero essere vulnerabili ad attacchi informatici come malware, ransomware o violazioni dei dati se non vengono correttamente protetti. Le vulnerabilità del software e i patch non applicate potrebbero esporre i server a rischi di sicurezza.

Rete wireless: Le reti wireless sono vulnerabili a varie forme di attacchi, tra cui attacchi di spoofing, sniffing di pacchetti e accesso non autorizzato. La mancanza di crittografia forte, autenticazione debole o configurazioni di rete non sicure potrebbero compromettere la sicurezza della rete wireless.

Dispositivi personali non adeguatamente protetti: I dispositivi personali utilizzati dai dipendenti potrebbero mancare di adeguati controlli di sicurezza, esponendo l'azienda a rischi come malware, accesso non autorizzato o perdita di dati.

Dispositivi personali (BYOD): I dispositivi personali utilizzati dai dipendenti rappresentano una potenziale minaccia per la sicurezza se non vengono adeguatamente gestiti.

Politiche BYOD non sufficientemente rigorose: Le politiche BYOD potrebbero essere troppo permissive o non essere applicate in modo uniforme, aumentando il rischio di compromissione dei dati sensibili.

2.3. Vulnerabilità legate alla sicurezza dei dati:

Laptop e workstation per sviluppatori e consulenti: I dispositivi utilizzati dai dipendenti per lo sviluppo software potrebbero essere vulnerabili a minacce come attacchi di phishing, malware o perdita fisica. È importante implementare misure di sicurezza come l'antivirus, la crittografia dei dati e le politiche di accesso per proteggere questi dispositivi.

Difese inadeguate contro attacchi informatici: Le misure di sicurezza come firewall, antivirus e sistemi di rilevamento delle intrusioni potrebbero essere insufficienti o non aggiornate, rendendo l'azienda vulnerabile a varie forme di attacchi informatici.

Manutenzione e backup dei dati non ottimali: I processi di backup potrebbero non essere eseguiti regolarmente o non essere testati in modo adeguato, aumentando il rischio di perdita di dati in caso di violazioni o guasti dei sistemi.

Filiali regionali: Se le filiali regionali hanno infrastrutture IT proprie, potrebbero essere vulnerabili a minacce simili a quelle della sede centrale. È importante estendere le misure di sicurezza a tutte le filiali e garantire una gestione centralizzata della sicurezza.

2.4. Vulnerabilità legate alla conformità normativa:

Non conformità alle normative sulla protezione dei dati: Potrebbero mancare procedure e controlli adeguati per garantire la conformità alle normative sulla protezione dei dati come il GDPR, esponendo l'azienda a rischi legali e finanziari.

2.5. Vulnerabilità legate alla gestione dei rischi:

Assenza di piani di risposta agli incidenti: Potrebbe mancare un piano formale per gestire incidenti di sicurezza come violazioni dei dati o attacchi informatici, aumentando il rischio di danni prolungati e costosi.

2.6. Vulnerabilità legate alla formazione del personale:

Mancanza di formazione sulla sicurezza informatica: Il personale potrebbe non essere adeguatamente istruito su pratiche di sicurezza informatica e sulle politiche aziendali, aumentando il rischio di comportamenti non sicuri o inconsapevoli.

2.7. Vulnerabilità legate alla sicurezza del cloud:

Cloud pubblici (AWS, Azure): Anche se i provider di servizi cloud come AWS e Azure offrono misure di sicurezza robuste, la configurazione errata delle risorse cloud potrebbe esporre l'azienda a rischi. Ad esempio, le credenziali di accesso deboli o la configurazione non sicura delle autorizzazioni potrebbero portare a violazioni dei dati.

Configurazioni errate o inadeguate: Le configurazioni di sicurezza dei servizi cloud potrebbero non essere ottimali, esponendo l'azienda a rischi come violazioni dei dati o accesso non autorizzato.

2.8. Vulnerabilità legate alla gestione dei rischi finanziari:

Mancanza di assicurazione cibernetica: Potrebbe mancare un'adeguata copertura assicurativa contro le violazioni dei dati e altri incidenti di sicurezza, aumentando il rischio di perdite finanziarie in caso di incidente.

2.9. Vulnerabilità legate alla reputazione:

Mancanza di gestione della comunicazione durante gli incidenti: In caso di violazioni dei dati o altri incidenti di sicurezza, potrebbe mancare una comunicazione tempestiva e trasparente con i clienti e le parti interessate, aumentando il rischio di danni alla reputazione.

Perdita di fiducia**:** Se gli Stakeholders(i clienti, i partner commerciali e gli utenti) sono vittime di attacchi, potrebbero perdere fiducia nell'organizzazione che sembra non essere in grado di proteggere adeguatamente i loro dati. Ciò può portare a una perdita di reputazione e alla riduzione della clientela.

La TechnoCorp deve affrontare una serie di vulnerabilità potenziali in vari aspetti della sua infrastruttura IT. Implementare misure di sicurezza robuste e una rigorosa politica di gestione della sicurezza delle informazioni è fondamentale per mitigare questi rischi e proteggere l'azienda da possibili minacce.

3. Analisi delle minacce

L'analisi delle minacce potenziali che TechnoCorp potrebbe affrontare:

3.1 Attacchi informatici:

Questa è una minaccia chiave per TechnoCorp, data la natura del settore in cui opera. Gli attacchi informatici possono provenire da attaccanti esterni, come hacker o gruppi criminali, che potrebbero mirare a violare i dati sensibili dell'azienda o interrompere le operazioni aziendali.

1. **Malware e ransomware:** Gli attacchi malware, compresi quelli che impiegano ransomware, sono una minaccia costante per TechnoCorp. Tali attacchi possono causare la perdita di dati, la compromissione dei sistemi aziendali e il blocco delle operazioni aziendali fino al pagamento del riscatto.
2. **Exploit di vulnerabilità del software:** Le vulnerabilità del software nei server interni, nei servizi cloud utilizzati e nel sito web aziendale ospitato esternamente potrebbero essere sfruttate dagli attaccanti per ottenere accesso non autorizzato ai sistemi o per compromettere i dati aziendali.
3. **Violazioni della sicurezza dei dati:** La perdita o la compromissione dei dati sensibili dell'azienda o dei suoi clienti rappresenta una minaccia significativa. Le

violazioni della sicurezza dei dati possono causare danni alla reputazione dell'azienda, sanzioni legali e perdite finanziarie.

4. **Accesso non autorizzato:** Gli attaccanti potrebbero cercare di ottenere accesso non autorizzato ai sistemi aziendali attraverso vulnerabilità della rete, credenziali rubate o altri mezzi. Questo potrebbe consentire loro di rubare dati sensibili, interrompere le operazioni aziendali o causare danni alla reputazione dell'azienda. Un caso specifico è lo **Spoofing**, una tecnica in un cui un individuo o un programma falsifica l'identità di un'altra persona, sistema informatico o risorsa, al fine di ingannare gli utenti o ottenere accesso non autorizzato.
5. **Attacchi DDoS:** Gli attacchi distribuiti di denial of service (DDoS) possono interrompere le operazioni aziendali, rendendo inaccessibili i servizi aziendali online o le risorse critiche. Questi attacchi possono essere condotti da attaccanti esterni con l'obiettivo di danneggiare l'azienda o estorcere denaro.
6. **USB Drop Attacks:** Gli attaccanti lasciano dispositivi USB infetti con malware in luoghi pubblici o all'interno dell'azienda stessa, contando sulla curiosità delle persone per inserire i dispositivi nei propri computer, consentendo così l'infezione.

3.2 Attacchi di **social engineering** & **HUMINT**:

1. **Phishing**: Gli attacchi di phishing rappresentano una minaccia significativa, in particolare per i dipendenti, gli attaccanti potrebbero cercare di ottenere accesso non autorizzato alle credenziali aziendali o di distribuire malware attraverso e-mail di phishing mirate. Nel caso specifico dello **Spear Phishing** gli attaccanti mirano a persone o organizzazioni specifiche, utilizzando informazioni precedentemente raccolte per rendere gli attacchi più convincenti e credibili.
2. **Vishing**: Gli attaccanti utilizzano telefonate ingannevoli verso gli uffici aziendali per convincere i dipendenti a condividere informazioni riservate, effettuare pagamenti non autorizzati o scaricare malware sui loro dispositivi.

3. **Infiltrazione fisica**: Gli attaccanti si fingono appartenenti al personale di manutenzione, consegna o altro personale esterno per ottenere accesso fisico non autorizzato a strutture o sistemi aziendali sensibili.
4. **Tailgating**: Gli attaccanti seguono un dipendente autorizzato attraverso l'accesso fisico controllato, come una porta con badge, sfruttando la cortesia o la mancanza di attenzione per guadagnare accesso non autorizzato alle strutture o ai sistemi aziendali.
5. **Smishing**: Gli attaccanti inviano messaggi di testo fraudolenti o ingannevoli alle vittime con lo scopo di ottenere dati sensibili, o indurre l'utente a compiere azioni dannose, come il download di contenuti o l'apertura di siti malevoli.
6. **Deepfake**: Gli attaccanti utilizzano (manipolazione di video, falsificazione di discorsi, truffe on-linee, attacchi di phishing avanzati, falsificazione di prove) per creare video o registrazioni manipolate artificialmente in modo che sembri che una persona stia facendo qualcosa che in realtà non ha fatto.

3.3 Disastri ed eventi naturali naturali:

1. **Eventi meteorologici estremi:** Tempeste, uragani, alluvioni, terremoti e altre calamità naturali possono danneggiare fisicamente gli edifici, gli impianti e le infrastrutture dell'azienda IT. Questo potrebbe causare interruzioni dei servizi, perdita di dati e danni ai sistemi critici.

2. **Incendi**: Gli incendi possono distruggere attrezzature, server e infrastrutture di rete, causando interruzioni dei servizi e perdita di dati. La presenza di apparecchiature elettriche e dispositivi informatici all'interno di un'azienda IT aumenta il rischio di incendi, che possono essere causati da cortocircuiti, surriscaldamento o guasti hardware.

3. **Blackout e interruzioni dell'alimentazione elettrica:** Interruzioni di corrente a lungo termine o blackout possono influenzare gravemente le operazioni di un'azienda IT, causando la perdita di dati non salvati, l'interruzione dei servizi e danni alle apparecchiature elettriche sensibili.

3.4 Altri tipi di minacce:

1. **Minacce esterne**: Se un dispositivo personale viene compromesso durante l'utilizzo personale, potrebbe consentire a un attaccante di ottenere accesso non autorizzato alle risorse aziendali.
2. **Perdita fisica dei dispositivi**: La perdita o il furto di laptop, workstation o altri dispositivi aziendali potrebbe compromettere la sicurezza dei dati aziendali se i dispositivi contengono informazioni sensibili e non sono adeguatamente protetti con misure di sicurezza come la crittografia dei dati.

4. Modellazione delle minacce

Per modellare le minacce in modo efficace, possiamo utilizzare il framework STRIDE, che identifica sei categorie principali di minacce alla sicurezza dell'informazione:

4.1 **Spoofing**:

Un attaccante si finge di essere un'altra entità per ottenere accesso non autorizzato ai sistemi o alle informazioni. Ad esempio, un attaccante potrebbe falsificare le credenziali di accesso per ottenere l'accesso ai server interni di TechnoCorp.

Potenziale Impatto sul Business:

Il grado di impatto potenziale del tampering sull'organizzazione può essere significativo e può includere i seguenti aspetti:

I. **Perdita di fiducia e reputazione:** Se i clienti, i partner commerciali o gli utenti interni sono vittime di spoofing, potrebbero perdere fiducia nell'organizzazione che sembra non essere in grado di proteggere adeguatamente i loro dati. Ciò può portare a una perdita di reputazione e alla riduzione della clientela.

II. **Violazione della sicurezza dei dati sensibili:** Lo spoofing può consentire agli aggressori di accedere a informazioni riservate o sensibili dell'organizzazione, come dati finanziari, informazioni personali dei clienti o proprietà intellettuale.

Questo può portare a violazioni della conformità normativa e a conseguenti sanzioni legali.

III. **Perdite finanziarie:** Gli attacchi di spoofing possono essere utilizzati per ingannare gli utenti interni dell'organizzazione o i fornitori a compiere azioni dannose, come il trasferimento di fondi o l'accesso non autorizzato a sistemi critici. Questo può portare a gravi perdite finanziarie per l'organizzazione.

IV. **Interruzione delle operazioni aziendali:** Se un attacco di spoofing è sufficientemente sofisticato da compromettere l'accesso ai sistemi critici o ai dati aziendali, potrebbe causare interruzioni significative nelle operazioni quotidiane dell'organizzazione. Ciò potrebbe comportare la perdita di produttività, la mancata erogazione di servizi e la conseguente perdita di entrate.

V. **Costi aggiuntivi per la sicurezza informatica:** Dopo un attacco di spoofing, un'organizzazione potrebbe essere costretta a investire in misure di sicurezza informatica aggiuntive per prevenire futuri incidenti. Ciò potrebbe includere l'implementazione di soluzioni di autenticazione più robuste, la formazione del personale sulla sicurezza informatica e la revisione delle politiche e delle procedure aziendali.

4.2 **Tampering** (Alterazione):

Il tampering è una minaccia che comporta la manipolazione o l'alterazione non autorizzata di dati, sistemi o risorse all'interno di un'organizzazione. Gli attaccanti possono cercare di alterare informazioni sensibili, codice sorgente, configurazioni di sistema o dispositivi hardware al fine di compromettere l'integrità, la disponibilità o la riservatezza dei dati e dei sistemi.

Potenziale Impatto sul Business:

I. **Perdita di Integrità dei Dati:** La manomissione dei dati può compromettere l'integrità delle informazioni critiche per l'organizzazione, come dati finanziari,

transazioni commerciali o record dei clienti, compromettendo la fiducia dei clienti e causando danni all'immagine aziendale.

II. **Violazione della Compliance:** La manipolazione non autorizzata dei dati può portare a violazioni delle normative sulla privacy dei dati, come il GDPR o l'HIPAA, con conseguenze legali e sanzioni finanziarie significative per l'organizzazione.

III. **Danni all'Operatività dei Sistemi:** La manomissione dei sistemi o del codice sorgente critico può causare malfunzionamenti o interruzioni dei servizi aziendali, compromettendo l'operatività e la continuità aziendale.

IV. **Perdita di Fiducia dei Clienti**

V. **Perdita di Dati Sensibili:** La manomissione dei dati sensibili può portare alla perdita o alla divulgazione non autorizzata di informazioni riservate dell'organizzazione, con conseguenze finanziarie e legali significative.

VI. **Rischio di Responsabilità Legale**: L'alterazione dei dati o dei sistemi può esporre l'organizzazione a rischi di responsabilità legale da parte dei clienti, dei partner commerciali o delle autorità di regolamentazione per danni derivanti da perdite di dati o interruzioni dei servizi.

4.3 **Repudiation** (Repudio):

Un attaccante tenta di negare o mascherare le proprie azioni, rendendo difficile identificare l'autore dell'attacco o le attività dannose. Ad esempio, un attaccante potrebbe eliminare le tracce di accesso ai server interni per mascherare il proprio coinvolgimento in un'attività illegale.

Potenziale Impatto sul Business:

I. **Integrità dei dati e transazioni**: Il repudio può compromettere l'integrità delle transazioni e dei dati all'interno di un sistema. Se un utente nega di aver eseguito un'azione, ad esempio una transazione finanziaria, potrebbe esserci una mancanza di prova per dimostrare altrimenti, mettendo a rischio l'integrità delle registrazioni.

II. **Affidabilità e fiducia:** Il repudio può minare la fiducia e l'affidabilità del sistema e degli utenti. Se gli utenti possono negare le loro azioni, diventa difficile per l'azienda dimostrare la responsabilità delle azioni compiute all'interno del sistema, compromettendo così la fiducia degli utenti e dei clienti nell'affidabilità del sistema.

III. **Conformità normativa:** Il repudio può avere implicazioni significative per la conformità normativa, specialmente in settori altamente regolamentati come il settore finanziario o sanitario. Le normative possono richiedere che le aziende siano in grado di dimostrare in modo affidabile chi ha eseguito determinate azioni all'interno del sistema, e il repudio può mettere a rischio la conformità normativa.

IV. **Responsabilità legale:** Il repudio può portare a dispute legali tra le parti coinvolte. Senza prove chiare e affidabili delle azioni compiute, le aziende potrebbero trovarsi in situazioni di responsabilità legale, ad esempio in caso di contestazioni di transazioni finanziarie o di accesso non autorizzato ai dati sensibili.

4.4 **Information Disclosure** (Divulgazione di informazioni):

Un attaccante accede o divulga informazioni sensibili o riservate senza autorizzazione. Questo potrebbe includere la visualizzazione dei dati dei clienti memorizzati nei server interni o la divulgazione di informazioni aziendali riservate tramite attacchi di phishing.

Potenziale Impatto sul Business:

La divulgazione non autorizzata di informazioni sensibili, nota come "Information Disclosure", può avere un impatto significativo sull'azienda, influenzando diversi aspetti chiave:

I. **Violazione della privacy dei clienti e dei dipendenti:** Se dati sensibili dei clienti o dei dipendenti vengono divulgati senza autorizzazione, l'azienda potrebbe violare le normative sulla privacy, come il GDPR in Europa o leggi sulla protezione dei dati in altri paesi. Ciò potrebbe portare a multe e sanzioni finanziarie, nonché a perdite di fiducia da parte dei clienti.

II. **Perdita di fiducia e reputazione:** La divulgazione non autorizzata di informazioni può danneggiare gravemente la reputazione dell'azienda. La perdita di fiducia dei clienti e dei partner commerciali può causare una diminuzione delle vendite, un aumento del churn rate e un impatto negativo sulla percezione pubblica dell'azienda.

III. **Violazione della proprietà intellettuale:** Se informazioni aziendali riservate vengono divulgate, ad esempio progetti di ricerca e sviluppo, segreti commerciali o strategie di marketing, l'azienda potrebbe subire danni finanziari significativi. La concorrenza potrebbe approfittare di queste informazioni per ottenere vantaggi competitivi, riducendo così la capacità dell'azienda di innovare e crescere.

IV. **Rischio di furto di identità e frode:** Se dati personali sensibili, come informazioni finanziarie o di identificazione personale, vengono divulgati, i clienti potrebbero diventare vittime di frodi finanziarie o di furto di identità. Ciò potrebbe portare a costi aggiuntivi per l'azienda sotto forma di risarcimenti, monitoraggio delle violazioni e assistenza alle vittime.

V. **Impatto legale e conformità normativa:** La divulgazione non autorizzata di informazioni potrebbe mettere l'azienda in violazione di leggi e regolamenti specifici del settore, comportando azioni legali da parte dei clienti, delle autorità di regolamentazione o delle autorità giudiziarie. Le conseguenze legali possono includere multe, azioni legali da parte dei clienti e danni all'immagine aziendale.

4.5 **Distributed Denial of Service** (DDoS):

Piu' attaccanti tentano di interrompere o ridurre l'accesso legittimo ai servizi aziendali, rendendo i sistemi inaccessibili o inutilizzabili per gli utenti autorizzati. Ad esempio, un attaccante potrebbe lanciare un attacco DDoS contro il sito web aziendale ospitato esternamente, rendendolo inaccessibile agli utenti legittimi.

Potenziale Impatto sul Business:

I. **Interruzione dei servizi:** Un attacco DDoS può interrompere i servizi online di un'organizzazione, rendendo il sito web o l'applicazione web inaccessibili agli

utenti legittimi. Questo può causare perdite di entrate se l'azienda dipende da tali servizi per le vendite o per la fornitura di servizi ai clienti.

II. **Perdita di reputazione:** Gli utenti possono percepire negativamente un'organizzazione che non è in grado di fornire accesso ai propri servizi online. La perdita di reputazione può danneggiare a lungo termine la fiducia dei clienti nell'azienda e influenzare negativamente le decisioni di acquisto future.

III. **Costi operativi aggiuntivi:** Combattere un attacco DDoS richiede risorse e tempo. Le organizzazioni possono dover investire in soluzioni di mitigazione degli attacchi DDoS, come servizi di protezione cloud o hardware dedicato, aumentando così i costi operativi.

IV. **Perdite finanziarie dirette:** Se un'organizzazione subisce un'interruzione dei servizi a causa di un attacco DDoS, potrebbe incorrere in perdite finanziarie dirette, ad esempio mancate entrate o penali dovute alla violazione di accordi di livello di servizio (SLA) con i clienti.

V. **Vulnerabilità a ulteriori attacchi:** Gli attacchi DDoS possono essere utilizzati come diversivo per altri tipi di intrusioni informatiche, come tentativi di furto di dati sensibili o compromissione dei sistemi interni dell'organizzazione. Questo potrebbe portare a ulteriori danni finanziari e di reputazione.

4.6 **Elevation of Privilege** (Aumento dei privilegi):

Un attaccante ottiene accesso non autorizzato a risorse o funzionalità a cui non dovrebbe avere accesso, aumentando i propri privilegi nel sistema. Ad esempio, un attaccante potrebbe sfruttare una vulnerabilità del software per ottenere accesso amministrativo ai server interni di TechnoCorp.

Potenziale impatto sul business :

I. **Compromissione della sicurezza dei dati:** Se un attaccante ottiene accesso amministrativo non autorizzato ai server interni o ad altre risorse critiche, potrebbe compromettere la sicurezza dei dati sensibili dell'azienda. Ciò potrebbe

portare alla divulgazione non autorizzata di informazioni sensibili, alla manipolazione dei dati o al furto di dati aziendali o dei clienti.

II. **Interruzione delle operazioni aziendali:** L'aumento dei privilegi potrebbe consentire agli attaccanti di interrompere le operazioni aziendali, ad esempio attraverso la cancellazione o la modifica di file critici, la disattivazione dei sistemi o l'interruzione dei servizi aziendali. Questo potrebbe causare perdite finanziarie dovute a tempi di inattività, ripristini dei sistemi e perdita di produttività.

III. **Violazione della conformità e delle normative:** Se un attaccante ottiene accesso amministrativo a sistemi che contengono dati soggetti a regolamentazioni specifiche, come informazioni finanziarie o dati personali dei clienti, l'azienda potrebbe violare le normative sulla privacy e la conformità normativa. Ciò potrebbe portare a multe e sanzioni legali significative.

IV. **Danno alla reputazione e perdita di fiducia dei clienti:** Una violazione della sicurezza che porta all'aumento dei privilegi potrebbe danneggiare gravemente la reputazione dell'azienda e la fiducia dei clienti. La pubblicità negativa e la perdita di clienti a seguito di una violazione della sicurezza potrebbero avere un impatto duraturo sull'azienda e sul suo successo futuro.

V. **Costi di ripristino e di risposta agli incidenti:** Dopo un attacco di aumento dei privilegi, l'azienda potrebbe dover affrontare costi significativi per ripristinare i sistemi, migliorare la sicurezza e rispondere agli incidenti. Ciò potrebbe includere l'implementazione di nuove misure di sicurezza, la revisione dei processi e delle procedure, nonché l'assistenza legale e forense.

5. Scenari di rischio

Gli scenari di rischio che potrebbero minacciare la sicurezza delle informazioni di TechnoCorp sono stati identificati dalle 6 macro categorie della modellizzazione delle minacce, riportiamo di seguito un esempio per ognuna di queste:

5.1 Spoofing

Attacco di phishing contro i dipendenti: Un attaccante invia e-mail di phishing ai dipendenti di TechnoCorp, fingendosi di essere un' amministrazione aziendale o un'altra entità fidata. Se un dipendente clicca su un link dannoso o condivide le proprie credenziali, l'attaccante potrebbe ottenere accesso non autorizzato ai sistemi aziendali o ai dati sensibili.

5.2 Tampering

Vulnerabilità del software nei server interni: Un attaccante sfrutta una vulnerabilità del software nei server interni di TechnoCorp per ottenere accesso non autorizzato ai dati sensibili o per compromettere l'integrità dei sistemi. Ad esempio, potrebbero sfruttare una vulnerabilità non patchata per eseguire un attacco di injection SQL e accedere ai database aziendali.

5.3 Information Disclosure

Perdita fisica di un laptop aziendale: Un dipendente di TechnoCorp perde un laptop aziendale contenente dati sensibili sui clienti e progetti aziendali. Se il laptop non è protetto da password o se i dati non sono criptati, un attaccante potrebbe accedere facilmente alle informazioni aziendali e compromettere la sicurezza dei dati.

5.4 Distributed Denial of Service

Attacco DDoS contro il sito web aziendale: Un gruppo di attaccanti avvia un attacco DDoS contro il sito web di TechnoCorp ospitato esternamente, saturando il server web con un'elevata quantità di traffico illegittimo. Questo rende il sito web inaccessibile agli utenti legittimi e danneggia la reputazione dell'azienda.

5.5 Repudiation

Compromissione delle credenziali di accesso ai servizi cloud: Un attaccante riesce a ottenere le credenziali di accesso a un servizio cloud utilizzato da TechnoCorp (come AWS o Azure) attraverso attacchi di phishing o furti di credenziali. Con queste credenziali, potrebbero

accedere ai dati aziendali sensibili memorizzati nel cloud e compromettere la sicurezza delle informazioni.

5.6 Elevation of privilege

Accesso non autorizzato alla rete wireless aziendale: Un attaccante sfrutta una vulnerabilità nella configurazione della rete wireless aziendale di TechnoCorp per ottenere accesso non autorizzato alla rete interna dell'azienda. Una volta all'interno della rete, potrebbero esplorare i sistemi e i dati sensibili o lanciare attacchi mirati contro altri dispositivi sulla rete.

6. Analisi qualitativa

Per condurre un'analisi qualitativa del rischio per TechnoCorp, possiamo valutare le minacce identificate considerando la loro probabilità di occorrenza e l'entità del danno potenziale. Utilizzeremo una scala qualitativa per valutare questi fattori e determinare il livello di rischio associato a ciascuna minaccia

Ecco un'analisi qualitativa di alcune minacce:

6.1 Attacco di phishing contro i dipendenti:

- Probabilità di occorrenza: *Alta*
- Danno potenziale: *Moderato-alto*
- Livello di rischio: *Alto*
- Descrizione: Gli attacchi di phishing sono comuni e possono avere un impatto significativo se hanno successo nel compromettere le credenziali o diffondere malware tra i dipendenti.

6.2 Vulnerabilità del software nei server interni:

- Probabilità di occorrenza: *Media*

- Danno potenziale: *Alto*
- Livello di rischio: *Medio-alto*
- Descrizione: Le vulnerabilità del software possono essere sfruttate dagli attaccanti per ottenere accesso non autorizzato ai dati sensibili o compromettere l'integrità dei sistemi aziendali.

6.3 Perdita fisica di un laptop aziendale:

- Probabilità di occorrenza: *Bassa-media*
- Danno potenziale: *Moderato-alto*
- Livello di rischio: *Medio*
- Descrizione: Anche se meno comune rispetto ad altre minacce, la perdita fisica/furto di un laptop aziendale potrebbe causare una compromissione della sicurezza dei dati se i dispositivi non sono adeguatamente protetti.

6.4 Attacco DDoS contro il sito web aziendale:

- Probabilità di occorrenza: *Bassa-media*
- Danno potenziale: *Variabile*
- Livello di rischio: *Medio*
- Descrizione: Gli attacchi DDoS possono essere sfruttati per interrompere le operazioni aziendali, anche se l'impatto dipende dalla durata e dall'intensità dell'attacco.

6.5 Compromissione delle credenziali di accesso ai servizi cloud:

- Probabilità di occorrenza: *Media*
- Danno potenziale: *Moderato-alto*

- Livello di rischio: *Medio-alto*
- Descrizione: La compromissione delle credenziali di accesso al cloud potrebbe consentire agli attaccanti di accedere ai dati sensibili aziendali memorizzati nel cloud.

6.6 Accesso non autorizzato alla rete wireless aziendale:

- Probabilità di occorrenza: *Media*
- Danno potenziale: *Moderato*
- Livello di rischio: *Medio*
- Descrizione: L'accesso non autorizzato alla rete wireless potrebbe consentire agli attaccanti di esplorare la rete aziendale e acquisire informazioni sensibili, ma l'impatto potrebbe essere mitigato con misure di sicurezza adeguate.

6.7 Attacco di ransomware contro i server interni:

- Probabilità di occorrenza: *Media*
- Danno potenziale: *Alto*
- Livello di rischio: *Medio-alto*
- Descrizione: Gli attacchi di ransomware ai server interni possono causare interruzioni significative delle operazioni aziendali e richiedere costose operazioni di ripristino dei dati.

Analizziamo più a fondo quest'ultimo scenario:

6.7.bis Attacco di ransomware contro i server interni

6.7.1 Stima della verosimiglianza

La stima della verosimiglianza secondo il framework NIST (National Institute of Standards and Technology) fornisce una valutazione della probabilità che una minaccia sfrutti una vulnerabilità specifica in un sistema o nell'ambiente di un'organizzazione.

Per determinare la verosimiglianza, si prendono in considerazione diversi fattori, tra cui la presenza e la diffusione della minaccia, la complessità e l'efficacia delle contromisure, e il grado di esposizione della vulnerabilità.

Basandosi sulle informazioni fornite:

- La minaccia di violazione dei dati sembra essere elevata, considerando l'importanza dei dati sensibili gestiti dall'azienda e la frequenza delle violazioni dei dati nell'ambiente cloud.
- Le contromisure di sicurezza possono essere implementate, ma la complessità del sistema cloud potrebbe rendere difficile la gestione di tutte le vulnerabilità.
- L'esposizione alla vulnerabilità potrebbe essere significativa, data la complessità del sistema cloud e il numero potenziale di punti di accesso.

Basandosi sulla stima che la probabilità di un incidente di questo tipo sia del “Media” (50%), secondo la seguente tabella il livello di verosimiglianza è “Moderata” - “Se l'evento di minaccia viene avviato o si verifica, è probabile che abbia effetti negativi”.

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.

6.7.2 Stima dell'impatto

Basandosi sul calcolo effettuato sopra del report l'impatto relativo alla perdita dei dati sul business dell'azienda, secondo la seguente tabella il livello d'impatto è "Alto"- "*Si potrebbe prevedere che l'evento minaccioso abbia un effetto negativo grave o catastrofico operazioni organizzative, beni organizzativi, individui, altre organizzazioni o la Nazione. UN effetto avverso grave o catastrofico significa che, ad esempio, l'evento minaccioso potrebbe:*

(i) causare a grave degrado o perdita della capacità della missione nella misura e nella durata dell'organizzazione non in grado di svolgere una o più delle sue funzioni primarie;

(ii) provocare gravi danni a asset organizzativi;

(iii) comportare gravi perdite finanziarie;

(iv) provocare danni gravi o catastrofici a persone che comportano la morte o lesioni gravi mortali."

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.

6.7.3 Stima del rischio

Sfruttando le tabelle dei due punti precedenti e, applicando i risultati alla tabella seguente, si può stimare il grado di rischio che come possiamo vedere è "*Moderato*".

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

6.7.4 Descrizione del rischio

"Moderato" significa che ci si può aspettare che un evento minaccioso abbia un effetto negativo limitato operazioni organizzative, beni organizzativi, individui, altre organizzazioni o la Nazione.

TABLE I-3: ASSESSMENT SCALE – LEVEL OF RISK

Qualitative Values	**Semi-Quantitative Values**		**Description**
Very High	96-100	10	**Very high risk** means that a 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	**High risk** means that a threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Moderate	21-79	5	**Moderate risk** means that a threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Low	5-20	2	**Low risk** means that a threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Very Low	0-4	0	**Very low risk** means that a threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

Grazie!