

RISK MANAGEMENT

IDENTIFICAZIONE

E ANALISI DEL

RISCHIO

MARIA HUAPAYA



INDICE

Traccia

1. Introduzione

- Presentazione dell'azienda TechnoCorp
- Descrizione del settore IT e dei servizi IT
- Breve storia dell'azienda e dimensioni

2. Infrastruttura IT

- Descrizione dettagliata dell'infrastruttura IT
- Schema di rete

3. Clienti e Dati Sensibili

- Tipi di dati sensibili gestiti da TechnoCorp
- Profilo dei principali clienti

4. Personale e Accessi

- Descrizione dei vari ruoli e dei relativi livelli di accesso all'infrastruttura IT
- Politiche di password e autenticazione a due fattori

5. Scenario di Rischio 1 Top-down

- Identificazione del rischio
- Analisi del rischio semi-quantitativa
- Utilizzo delle tabelle G-4/H-3/I-2 del NIST SP 800-30 Rev. 1

6. Scenario di Rischio 2 Top-down

- Identificazione del rischio
- Analisi del rischio semi-quantitativa
- Utilizzo delle tabelle G-4/H-3/I-2 del NIST SP 800-30 Rev. 1

7. Scenario di Rischio 3 Bottom-up

- Identificazione del rischio
- Analisi del rischio semi-quantitativa
- Utilizzo delle tabelle G-4/H-3/I-2 del NIST SP 800-30 Rev. 1

8. Conclusioni

- Sintesi dei risultati dell'analisi del rischio
- Raccomandazioni preliminari per la mitigazione del rischio

9. Appendice

- Fonti note o studi di settore utilizzati per le probabilità di occorrenza, statistiche e stime



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.



INTRODUZIONE

Presentazione dell'azienda TechnoCorp

TechnoCorp è un'azienda leader nel settore delle tecnologie dell'informazione e dei servizi IT. Specializzata nella fornitura di consulenza, sviluppo software e gestione di infrastrutture tecnologiche, TechnoCorp serve un'ampia gamma di clienti in diverse industrie, sfruttando le sue competenze per offrire soluzioni innovative e su misura.

Descrizione del settore IT e dei servizi IT

Il settore delle tecnologie dell'informazione e dei servizi IT è altamente dinamico e competitivo, con una costante necessità di innovazione e aggiornamento tecnologico. Le aziende in questo settore devono affrontare sfide continue, tra cui la sicurezza dei dati, la gestione delle risorse IT e la necessità di adattarsi rapidamente ai cambiamenti tecnologici e alle esigenze dei clienti.

Breve storia dell'azienda e dimensioni

Fondata 15 anni fa, TechnoCorp ha cresciuto notevolmente la sua presenza nel mercato, espandendosi da una piccola start-up a un'azienda di medie dimensioni con circa 500 dipendenti.

Le tre filiali regionali supportano la sua operatività su scala nazionale.

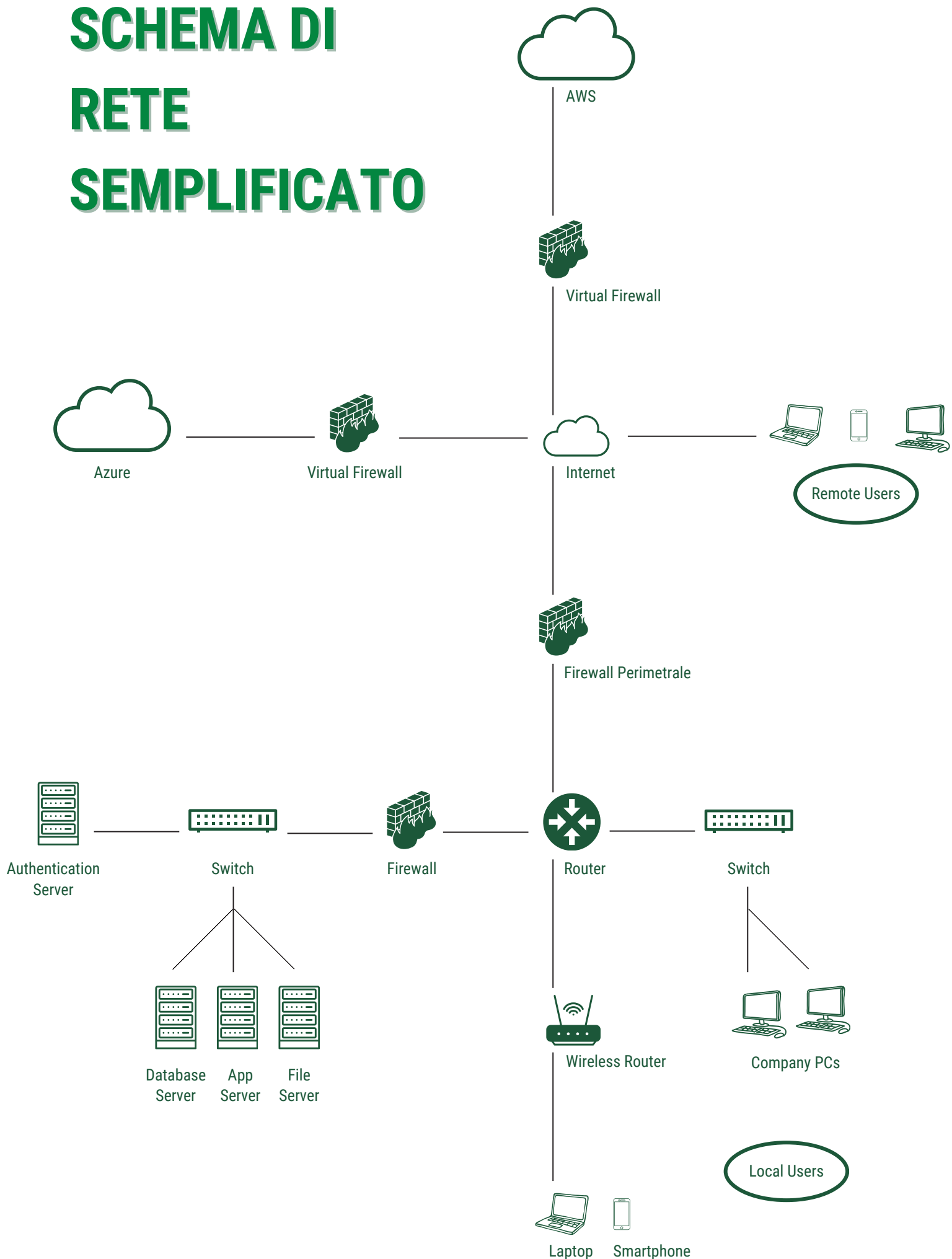
INFRASTRUTTURA IT

Descrizione dettagliata dell'infrastruttura IT

TechnoCorp si basa su un'infrastruttura IT complessa e diversificata per supportare le sue operazioni. Gli elementi chiave dell'infrastruttura includono:

- **Server Interni:** questi server ospitano applicazioni aziendali critiche, database, e sistemi di archiviazione dati. Sono il cuore del trattamento delle informazioni e della gestione delle operazioni di TechnoCorp.
- **Cloud Pubblici (AWS, Azure):** per alcune delle sue operazioni e servizi, TechnoCorp sfrutta le capacità dei cloud pubblici, permettendo una maggiore scalabilità e flessibilità delle sue risorse IT.
- **Rete Wireless:** gestita internamente per garantire connettività ai dipendenti e ai guest. Questa rete supporta anche i dispositivi personali e le workstation mobili attraverso un accesso controllato.
- **Dispositivi Personali (BYOD):** i dipendenti possono utilizzare i propri dispositivi per accedere a risorse aziendali attraverso la rete wireless, una pratica che aumenta la flessibilità ma introduce anche potenziali rischi di sicurezza.
- **Laptop e Workstation:** utilizzati principalmente da sviluppatori e consulenti, questi dispositivi sono essenziali per lo sviluppo di software e altre attività tecniche.
- **Sito Web Aziendale:** gestito e ospitato esternamente, serve come punto di contatto principale per clienti e partner, oltre a essere una risorsa critica per il marketing e la vendita dei servizi.
- **Firewall Perimetrale:** un componente critico per la sicurezza della rete, il firewall perimetrale protegge la rete interna da accessi non autorizzati e traffico potenzialmente dannoso.
- **EDR/xDR (Endpoint Detection and Response):** implementato su server, laptop, workstation e dispositivi personali, l'EDR/xDR fornisce monitoraggio continuo, rilevazione delle minacce e capacità di risposta agli incidenti.

SCHEMA DI RETE SEMPLIFICATO



CLIENTI E DATI SENSIBILI

Tipi di dati sensibili gestiti da TechnoCorp

TechnoCorp gestisce una vasta gamma di dati sensibili che sono cruciali sia per le operazioni interne sia per i servizi offerti ai clienti. Questi dati includono:

- **Informazioni Finanziarie:** TechnoCorp processa e memorizza dettagli finanziari significativi sia per la propria gestione che per quella dei clienti, come informazioni bancarie e transazioni.
- **Dati Personali di Dipendenti e Clienti:** comprende tutto, dalle informazioni di contatto fino ai dati personali più sensibili come il numero di previdenza sociale e dettagli di salute, particolarmente rilevanti per clienti nel settore sanitario.
- **Proprietà Intellettuale:** questo include dati e informazioni legate a brevetti, processi aziendali interni, software sviluppato su misura e altre forme di conoscenza critica esclusiva dell'azienda e dei suoi clienti.

Profilo dei Principali Clienti

I principali clienti di TechnoCorp includono istituzioni in diversi settori altamente regolamentati e che richiedono elevati standard di sicurezza e privacy:

- **Banche:** gestiscono enormi quantità di dati finanziari sensibili e sono soggette a rigide normative sulla protezione dei dati.
- **Compagnie di Assicurazioni:** richiedono la gestione di dati personali e finanziari su vasta scala, necessitando di robuste misure di sicurezza per proteggere tali informazioni.
- **Aziende Sanitarie:** hanno esigenze particolari relative alla protezione dei dati personali e sanitari dei pazienti, regolati da specifici standard e leggi sulla privacy.
- **Produttori:** spesso coinvolgono la protezione della proprietà intellettuale e dati relativi a innovazioni tecniche e di prodotto.

PERSONALE E ACCESSI

Descrizione dei vari ruoli e dei relativi livelli di accesso all'infrastruttura IT

TechnoCorp implementa una politica di accesso differenziato basata sul principio di minimo privilegio per garantire che il personale acceda solo alle risorse necessarie per svolgere le proprie funzioni. Ecco come sono distribuiti i livelli di accesso tra i vari ruoli:

- **Amministratori di Sistema:** hanno accesso completo a tutta l'infrastruttura IT, compresi i server critici e i sistemi di backup. Questo livello di accesso consente loro di eseguire compiti di manutenzione e aggiornamento essenziali per la sicurezza e l'efficienza operativa.
- **Sviluppatori:** accedono ai sistemi di sviluppo e alle piattaforme di test per creare e testare nuove applicazioni e aggiornamenti software. L'accesso è generalmente limitato agli ambienti di sviluppo per evitare rischi per i sistemi operativi critici.
- **Personale di Supporto Tecnico:** ha accesso limitato ai sistemi, necessario per assistere gli utenti finali e risolvere problemi relativi alle postazioni di lavoro e ai dispositivi mobili. Non hanno accesso ai server centrali o ai database principali.
- **Consulenti e Collaboratori Esterni:** ricevono credenziali temporanee o limitate, con accesso circoscritto alle aree di loro competenza. Queste credenziali sono monitorate strettamente e revocate non appena il lavoro è completato o in caso di interruzione della collaborazione.

Politiche di Password e Autenticazione a Due Fattori

TechnoCorp adotta una politica di password robusta e l'autenticazione a due fattori (2FA) per tutti gli accessi ai sistemi interni:

- **Politiche di Password:** richiedono la creazione di password complesse che includono una combinazione di lettere maiuscole, minuscole, numeri e simboli. Le password devono essere cambiate regolarmente.
- **Autenticazione a Due Fattori:** oltre alla password, è richiesto un secondo fattore di autenticazione, come un token hardware, un'app di autenticazione sul telefono o un messaggio SMS, per accedere ai sistemi aziendali.

SCENARIO DI RISCHIO 1

TOP-DOWN: INTERRUZIONE DEL SERVIZIO CLOUD PUBBLICO

Identificazione del Rischio

Questo scenario considera il rischio di una interruzione significativa nei servizi cloud (AWS, Azure) utilizzati da TechnoCorp. Tale interruzione può essere causata da vari fattori come attacchi DDoS, guasti tecnici o errori umani.

Analisi degli Asset

- **Asset Coinvolti:** infrastrutture cloud che ospitano applicazioni aziendali cruciali e dati sensibili dei clienti.
- **Valore degli Asset:** il fatturato dipendente dalle operazioni cloud è stimato a 200 milioni di euro, con circa il 70% delle operazioni aziendali che dipendono da queste infrastrutture.

Analisi delle Vulnerabilità

- **Dipendenza da Provider di Cloud Esterni:** la centralizzazione delle operazioni cruciali nei servizi cloud espone l'azienda a rischi di interruzioni di servizio.
- **Configurazioni di Sicurezza Non Adeguatamente Fortificate:** vulnerabilità nelle configurazioni possono esporre i servizi a attacchi informatici.

Analisi delle Minacce

- **Attacchi DDoS:** mirati a sovraccaricare i server cloud, causando interruzioni del servizio.
- **Guasti Tecnici o Errori Umani:** errori nella gestione delle infrastrutture cloud o guasti hardware/software possono causare downtime.

Modellazione delle Minacce

Utilizziamo il framework STRIDE per categorizzare le minacce, concentrando l'attenzione su:

- Denial of Service (DoS): incapacità di accedere ai servizi cloud.
- Tampering: manomissione dei dati a causa di configurazioni inadeguate.

Analisi del Rischio Semi-Quantitativa

- Probabilità: alta, dati i recenti attacchi su larga scala a provider di servizi cloud.
- Impatto: elevato, a causa dell'importanza critica dei servizi cloud per le operazioni aziendali.
- Esposizione al Fattore (EF): 40%, valutando che un'interruzione possa compromettere una parte significativa delle operazioni.
- Single Loss Expectancy (SLE):
 $200,000,000 \times 0.4 = 80,000,000$ euro.
- Annual Rate of Occurrence (ARO): 0.3, considerando la frequenza degli attacchi DDoS.
- Annual Loss Expectancy (ALE):
 $80,000,000 \times 0.3 = 24,000,000$ euro/anno.

Utilizzo delle Tabelle NIST SP 800-30 Rev. 1

- Tavola G-4 (Verosomiglianza): classificata come "Moderata" (50% probabilità) data la frequenza degli attacchi DDoS nei servizi cloud.

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.

- Tavola H-3 (Impatto sul Business): impatto "Elevato" (>€10M danni potenziali) a causa della dipendenza critica di TechnoCorp dai servizi cloud per le operazioni quotidiane.

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.

- Tavola I-2 (Livello di Impatto Complessivo): il rischio è valutato come "Alto", combinando la verosomiglianza moderata con un impatto elevato.

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

SCENARIO DI RISCHIO 2

TOP-DOWN: COMPROMISSIONE DEI DISPOSITIVI PERSONALI (BYOD)

Identificazione del Rischio

In questo scenario, il rischio è la compromissione dei dispositivi personali utilizzati dai dipendenti che potrebbe portare a una violazione dei dati sensibili dei clienti.

Analisi degli Asset

- Asset Coinvolti: dati sensibili dei clienti gestiti tramite dispositivi BYOD.
- Valore degli Asset: Stima di un contributo al fatturato annuo di 200 milioni di euro, con il 60% del fatturato influenzato dall'accesso ai dati dai dispositivi BYOD.

Analisi delle Vulnerabilità

- Mancanza di Controlli di Sicurezza Adeguati: dispositivi personali spesso non sono soggetti agli stessi controlli di sicurezza rigorosi come i dispositivi aziendali.
- Connessioni di Rete Non Sicure: connessioni non criptate o non protette possono essere sfruttate per accedere ai dati.

Analisi delle Minacce

- Malware/Phishing: attacchi che mirano a sottrarre credenziali o installare malware sui dispositivi personali.
- Perdita/Furto di Dispositivi: dispositivi personali contenenti dati sensibili possono essere persi o rubati, esponendo dati aziendali.

Modellazione delle Minacce

Focus su:

- Information Disclosure: rivelazione non autorizzata di informazioni a causa della compromissione di un dispositivo BYOD.

Analisi del Rischio Semi-Quantitativa

- Probabilità: alta, data la crescente sofisticatezza degli attacchi mirati ai dispositivi mobili e la diffusa adozione del BYOD.
- Impatto: elevato, per l'importanza dei dati sensibili accessibili tramite i dispositivi.
- Esposizione al Fattore (EF): 30%.
- Single Loss Expectancy (SLE):
 $200,000,000 \times 0.3 = 60,000,000$ euro.
- Annual Rate of Occurrence (ARO): 0.4.
- Annual Loss Expectancy (ALE):
 $60,000,000 \times 0.4 = 24,000,000$ euro/anno.

Utilizzo delle Tabelle NIST SP 800-30 Rev. 1

- **Tavola G-4:** la probabilità di compromissione dei dispositivi BYOD è considerata "Alta" (80% probabilità) per la crescente sofisticatezza e il numero di attacchi mirati ai dispositivi mobili.

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.

- **Tavola H-3:** l'impatto è "Elevato" (>€10M danni potenziali) considerando la quantità e il tipo di dati sensibili accessibili tramite dispositivi BYOD.

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.

- **Tavola I-2:** il rischio complessivo è classificato come "Elevato", per l'alta probabilità e l'alto impatto.

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

SCENARIO DI RISCHIO 3

BOTTOM-UP: COMPROMISSIONE DEL FIREWALL PERIMETRALE

Identificazione del Rischio

Questo scenario riguarda una potenziale compromissione del firewall perimetrale di TechnoCorp, che potrebbe permettere l'accesso non autorizzato a reti e dati aziendali.

Analisi degli Asset

- Asset Coinvolti: firewall perimetrale e tutti i sistemi e dati protetti da esso.
- Valore degli Asset: 200 milioni di euro, con il 70% del fatturato dipendente dalle operazioni protette dal firewall.

Analisi delle Vulnerabilità

- Configurazioni di Sicurezza Inadeguate: configurazioni del firewall non ottimizzate possono lasciare aperte vulnerabilità.
- Mancanza di Aggiornamenti e Patch: firewall non aggiornati sono suscettibili a nuovi tipi di attacchi.

Analisi delle Minacce

- Attacchi mirati al Firewall: tentativi di bypassare o compromettere il firewall per accedere alla rete interna.
- Insider Threats: minacce interne che possono sfruttare la conoscenza dei sistemi per compromettere il firewall.

Modellazione delle Minacce

Focus su:

- Tampering e Elevation of Privilege: manomissione del firewall per ottenere accessi non autorizzati o elevare i privilegi.

Analisi del Rischio Semi-Quantitativa

- Probabilità: media, vista la crescente frequenza di attacchi sofisticati mirati alle infrastrutture critiche.
- Impatto: elevato, data la critica natura dei dati e sistemi protetti dal firewall.
- Esposizione al Fattore (EF): 30%.
- Single Loss Expectancy (SLE):
 $200,000,000 \times 0.3 = 60,000,000$ euro.
- Annual Rate of Occurrence (ARO): 0.2.
- Annual Loss Expectancy (ALE):
 $60,000,000 \times 0.2 = 12,000,000$ euro/anno.

Utilizzo delle Tabelle NIST SP 800-30 Rev. 1

- **Tavola G-4:** classificata come "Moderata" (50% probabilità), riflettendo una frequenza moderata di attacchi mirati specificamente ai firewall aziendali.

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.

- **Tavola H-3:** impatto "Elevato" (>€10M danni potenziali), data l'importanza del firewall nella protezione delle reti e dei dati interni dell'azienda.

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.

- **Tavola I-2:** il livello di rischio complessivo è valutato "Alto", considerando l'importanza critica del firewall e la frequenza significativa degli attacchi.

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



CONCLUSIONI


Dopo un'approfondita valutazione dei rischi associati alla sicurezza delle informazioni di TechnoCorp, abbiamo identificato e analizzato vari scenari di rischio che potrebbero impattare significativamente le operazioni aziendali. Questi scenari includono la compromissione dei dispositivi personali (BYOD), l'attacco al firewall perimetrale e l'interruzione del servizio cloud. Ciascuno di questi scenari presenta sfide uniche e richiede misure di mitigazione specifiche per ridurre la probabilità di occorrenza e l'impatto potenziale.

Raccomandazioni per la Mitigazione del Rischio

- **Rafforzamento delle Politiche di Sicurezza:** implementare politiche di sicurezza più stringenti per i dispositivi BYOD, inclusa la crittografia obbligatoria dei dati e l'autenticazione a più fattori.
- **Miglioramento delle Configurazioni di Sicurezza del Firewall:** aggiornare e monitorare regolarmente le configurazioni del firewall per assicurarsi che siano ottimizzate contro le ultime minacce e vulnerabilità.
- **Incremento della Redondanza e della Resilienza del Cloud:** diversificare i fornitori di servizi cloud e implementare soluzioni di failover automatico per garantire la continuità operativa in caso di interruzione di uno dei servizi.
- **Formazione Continua dei Dipendenti:** organizzare sessioni di formazione regolari per i dipendenti su temi di sicurezza informatica per aumentare la consapevolezza e ridurre il rischio di attacchi phishing e malware.
- **Implementazione di Strumenti di Monitoraggio Avanzati:** utilizzare strumenti di sicurezza avanzati per monitorare continuamente la rete e identificare tempestivamente potenziali intrusioni o anomalie.
- **Piani di Risposta agli Incidenti:** rivedere e testare i piani di risposta agli incidenti per assicurare una risposta rapida ed efficace in caso di violazione della sicurezza.

Sintesi dei Risultati dell'Analisi del Rischio

Le analisi qualitative e semi-quantitative hanno evidenziato che TechnoCorp è esposta



a rischi significativi che potrebbero compromettere la sicurezza dei suoi dati sensibili e delle infrastrutture IT. Evidenziando la necessità di un approccio proattivo alla gestione del rischio, le raccomandazioni proposte mirano a rafforzare la resilienza dell'azienda contro le minacce identificate.

In conclusione, affrontare questi rischi con un approccio sistematico e integrato non solo proteggerà TechnoCorp da potenziali perdite finanziarie e danni alla reputazione, ma rafforzerà anche la fiducia dei clienti e partner commerciali nell'integrità delle sue operazioni.

Questa conclusione completa il nostro esame approfondito dei rischi di sicurezza di TechnoCorp. Se desideri ulteriori dettagli, aggiunte o modifiche al report, sono qui per assisterti nella finalizzazione del documento.



APPENDICE

Specifiche dei Server Interni

- Dettagli su hardware, capacità di storage, e configurazioni di sistema operativo.
- Informazioni su backup e misure di disaster recovery implementate.

Architettura dei Servizi Cloud

- Descrizione delle configurazioni di sicurezza specifiche per i servizi cloud AWS e Azure utilizzati.
- Politiche di accesso e gestione delle identità nei cloud pubblici.

Protocolli di Sicurezza per Rete Wireless e BYOD

- Standard di sicurezza implementati, inclusi WPA3 per la crittografia WiFi e soluzioni per la gestione delle identità digitali.
- Dettagli sulla segmentazione della rete e sulla separazione del traffico di rete per ospiti e dipendenti.

Procedure di Manutenzione e Aggiornamento del Firewall

- Frequenza degli aggiornamenti e delle revisioni di sicurezza per il firewall perimetrale.
- Dettagli sulle configurazioni delle politiche del firewall e delle liste di controllo degli accessi.

Panoramica su EDR/xDR

- Elenco di software e soluzioni EDR/xDR impiegati.
- Strategie di monitoraggio e risposta agli incidenti.

Fonti e Riferimenti

- NIST SP 800-30 Rev. 1: guida per le valutazioni del rischio, fornendo un framework per classificare e quantificare i rischi.
- ISO/IEC 27001: standard internazionale per la gestione della sicurezza delle informazioni.
- Relazioni di analisi del settore: Rapporti e white paper da parte di aziende di consulenza e analisti di settore relativi alle pratiche di sicurezza e ai recenti attacchi informatici.

Metodologie di Stima

- Stime delle Probabilità di Occorrenza: basate su dati storici di incidenti e analisi comparativa con organizzazioni simili nel settore.
- Valutazione dell'Impatto Finanziario: calcolo delle perdite potenziali utilizzando dati interni e benchmark di settore, inclusi costi diretti e indiretti delle violazioni dei dati.

GRAZIE

MARIA HUAPAYA

