Davide Andreozzi

BCC – Risk Management

Progetto settimanale
S01 – L05

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.

Identificazione del rischio

Dato il mercato in cui opera la TechnoCorp, gli asset aziendali e il valore finanziario dei dati dei clienti è stato identificato un potenziale rischio **generico** sulla sicurezza, in particolare potrebbero esserci delle violazioni dei dati sensibili dei clienti a causa di vulnerabilità nell'infrastruttura IT o accessi non autorizzati.

Procediamo successivamente ad un'analisi più dettagliata per identificare gli scenari di rischio specifici che l'azienda potrebbe dover affrontare e mitigare.

Analisi asset aziendali

Dati sensibili dei clienti

Clienti con richiesta di elevati standard di sicurezza, i dati in questione hanno un potere economico molto importante per queste aziende

Infrastruttura IT (server, cloud, rete, dispositivi)

Server interni con dati importanti (alta priorità)

Dispositivi aziendali non completamente gestiti dall'azienda

Firewall e dispositivi di controllo rete

Sito web aziendale

Il sito web aziendale è ospitato esternamente

Calcolo Asset

Asset	Valore stimato	Criticità (0-5)	Costi
Dati dei clienti	€ 16.650.000	5	€ 1.250.000 / Anno
Infrastruttura IT	€ 3.530.400	4	€ 135.000 / Anno
Sito Web aziendale	€ 35.000	2	€ 3.200 / Anno
Cloud (AWS, Azure)	€ 870.000	2	€ 7.000 / Anno

Analisi delle Vulnerabilità e delle Minacce

Vulnerabilità	Minaccia	Probabilità
Vulnerabilità non conosciute nei server interni, servizi cloud o nella rete wireless	Attacco informatico (Malware, DDoS, Exploit, Evil Twin)	Alta
Software non patchato	Rischio di Exploit Zero-Day	Bassa
Dipendenti o consulenti disonesti	Attivisti, concorrenti o criminali informatici potrebbero sfruttare del personale non contento o disonesto in cambio di pagamento per ottenere informazioni sensibili o l'accesso a risorse aziendali	Media
Dispositivi personali (BYOD)	Furto o perdita dei dispositivi contenenti informazioni riservate	Medio alta
Personale non adeguatamente formato	Rischio di phishing da parte di malintenzionati	Medio bassa

Modellazione delle minacce 1/2

Asset: Server interni

Vulnerabilità: Possibili vulnerabilità nei server interni, nei servizi cloud e nella rete wireless

Minaccia: Attacco informatico (Malware, DDoS, Exploit, Evil Twin)

Metodo d'attacco ipotetico: Esecuzione RCE su server interno.

Probabilità / Gravità: Alta

Contromisure:

Patchare gli applicativi, i server e tutti i sistemi informatici con le ultime patch di sicurezza disponibili (dopo testing per garantire la continuità del servizio).

Monitorare costantemente i log di firewall e degli endpoint, gestire correttamente le regole del firewall.

Implementare strategie di threat hunting per prepararsi a eventuali attacchi da organizzazioni criminali,

Implementare un team esterno che si occupi di Penetration Testing e Vulnerability Assesment.

Aggiornare e formare il personale contro gli attacchi di ingegneria sociale.

Modellazione delle minacce 2/2

Asset: Dispositivi personali (BYOD)

Vulnerabilità: Dispositivi personali non completamente controllati dall'azienda

Minaccia: perdita di informazioni riservate, rischio sanzioni da enti controllo privacy

Metodo d'attacco ipotetico: Accesso ai dati sensibili e informazioni aziendali presenti nei dispositivi personali (BYOD) dopo smarrimento o furto.

Probabilità / Gravità: Medio - Alta

Contromisure:

Crittografare i dati sensibili memorizzati sul dispositivo BYOD in modo che siano illeggibili per chiunque non abbia la chiave corrispondente, ciò fornisce una protezione aggiuntiva nel caso in cui i dati arrivino a fonti non autorizzate.

Implementare soluzioni di gestione dei dispositivi che consentano di monitorare, controllare e gestire i dispositivi BYOD da remoto.

Capacità di localizzare il dispositivo, bloccare o cancellare i dati in remoto.

Formazione, consapevolezza del rischio da parte del personale e politica di Backup rigorosa.

Scenari di rischio - Esecuzione RCE su server interno

L'attaccante esegue una scansione del server e delle applicazioni per individuare possibili falle di sicurezza.

Durante questo processo, scopre una vulnerabilità nel software del server che può essere sfruttata per l'esecuzione remota di codice, nonostante la presenza di firewall perimetrale, l'attore del attacco potrebbe sfruttare falle di configurazione, o tecniche di ingegneria sociale per entrare nella rete interna, oppure sfruttare del personale scontento.

Successivamente andrà ad eseguire codice arbitrario sul server per iniettare un ransomware che vada a replicarsi all'interno della rete aziendale oppure potrebbe compromettere i server più importanti per recuperare informazioni sensibili dei clienti per poterle vendere o renderle pubbliche, portando un danno d'immagine ed economico alla TechnoCorp

In base agli asset critici esposti e al danno d'immagine, le conseguenze a questo scenario porterebbero ad un danno economico enorme per la TechnoCorp, questo scenario di rischio presenta una priorità urgente per l'azienda.

Scenari di rischio - Accesso ai dati sensibili e informazioni aziendali presenti nei dispositivi personali

Il dispositivo viene rubato o smarrito, contiene accesso diretto alla rete aziendale e ai dati sensibili dei clienti.

Se il dispositivo non è adeguatamente protetto con una password o un meccanismo di autenticazione forte, il ladro potrebbe essere in grado di accedere ai dati sensibili memorizzati sul dispositivo.

Anche se il dispositivo è protetto da password, il ladro potrebbe tentare di bypassare la protezione utilizzando tecniche di cracking password o di recupero delle password abbinate a dell'ingegneria sociale.

Le conseguenze a questo scenario porterebbero ad un danno economico dovuto dalla perdita di fiducia da parte dei clienti e sanzioni da parte di enti governativi addetti al controllo della gestione dei dati personali e privacy.

Analisi Semi-quantitativa del rischio (RCE su Server interno)

1) Stime quantitative di un potenziale RCE su server interni
2) Stima della verosimiglianza
3) Stima dell’impatto
4) Stima del rischio
5) Descrizione del rischio

Stime quantitative di un potenziale RCE su server interni

Considerando il valore degli asset principali e la probabilità degli attacchi basati sulla tipologia e criticità delle informazioni nei server, insieme a un fatturato annuo di 75 milioni di euro, è stata effettuata un'analisi approfondita utilizzando diversi studi sugli attacchi informatici e la loro probabilità di successo.

Ad esempio, un'azienda che gestisce dati sensibili o critici, la probabilità di successo di un attacco informatico potrebbe essere considerata più alta rispetto a un'azienda meno esposta.

Probabilità evento = **75%**

Fatturato Annuo = **€ 75.000.000**

EF stimato: **45 %** (percentuale dell'asset che si prevede sarà persa in caso di evento

SLE = **€ 7.492.500**

La SLE è la singola perdita dovuta al verificarsi di una determinata minaccia

ARO = 4/1 = **4 attacchi/Anno**

L'ARO è la media con cui la minaccia si verifica annualmente

ALE = 7.492.500 * 4 = **€ 29.970.000/Anno**

L'ALE è la perdita stimata annualmente al verificarsi delle minacce

Impatto = 29.970.000/75.000.000*100 = **40 %**

L'impatto è il valore che identifica in termini economici quanto la minaccia incide sul fatturato annuo, possono essere quantificati anche ulteriori dati come il danno al brand, perdita di investitori, calo vendite, ecc.

Stima della verosimiglianza

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.

La probabilità del verificarsi dell'evento è del 75 % e presentiamo un rischio «Moderato», come indicato dalla tabella G-4

Stima dell’impatto

Il danno economico che gli eventi causerebbero all’azienda è di circa 30 Mln quindi il 40% del fatturato annuo.

Questo valore si classifica come «**Moderato**» sulla scala di valutazione dell’impatto che hanno le minacce

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

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

Il livello di rischio è dato dalla combinazione del livello di impatto e la probabilità che l'impatto si verifichi (verosimiglianza).
Ricapitolando, i valori per la nostra azienda sono:

- Verosimiglianza = *Moderate*
- Impatto = *Moderate*

Il livello di rischio dato dalla combinazione dei due valori precedenti sarà di «***Moderate***»

Successivamente andremo a vedere più nel dettaglio a cosa corrisponde il valore e come viene percepito.

Descrizione del rischio

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.

Descrizione del rischio

Dato il livello di rischio finale che abbiamo potuto vedere nella precedente slide come («**Moderate**»).

Ci si può aspettare che un evento minaccioso abbia un grave effetto negativo sulle operazioni organizzative, sugli asset organizzativi, sugli individui, altre organizzazioni o sulla nazione.

Questa valutazione del rischio ci informa che l'effetto verificatosi da un evento minaccioso come l'esecuzione di codice arbitrario su server interni possa mettere in serio pericolo gli asset organizzativi, la reputazione aziendale e l'operatività aziendale, portando ad un danno economico importante e conseguenze negative anche in termini di sanzioni e reputazione del brand.

E' quindi importante tenere costantemente sotto controllo le minacce e i scenari di rischio che potrebbero continuamente evolversi con un trend non prevedibile e implementare tutte le rimediation elencate in precedenza per eliminare o abbassare il livello del rischio su un valore che risulti accettabili per l'azienda in esame.