EPICODE

S2 - L5

Risk assessment

8 maggio 2024

Team

- Davide di Turo
- Manuel Di Gangi
- Marco Fasani

INDICE

Traccia

Simulare un processo di Risk Assessment, solo Step 1 e Step 2 (tralasciando Step 3 e Step 4), seguendo NIST SP 800-30, per Tier 3 (considerate solo le sorgenti del Tier 3). Riutilizzate la mappa delle relazioni tra tabelle, che avete prodotto ieri, come guida.

Siete liberi di impostare scopo, ambito, ipotesi e vincoli per limitare l'estensione del RA. Utilizzate gli step visti a lezione e definite solamente le tabelle essenziali che vi serviranno per il calcolo finale del rischio:

- D-7
- E-5
- F-3
- F-6
- H-4
- I-5

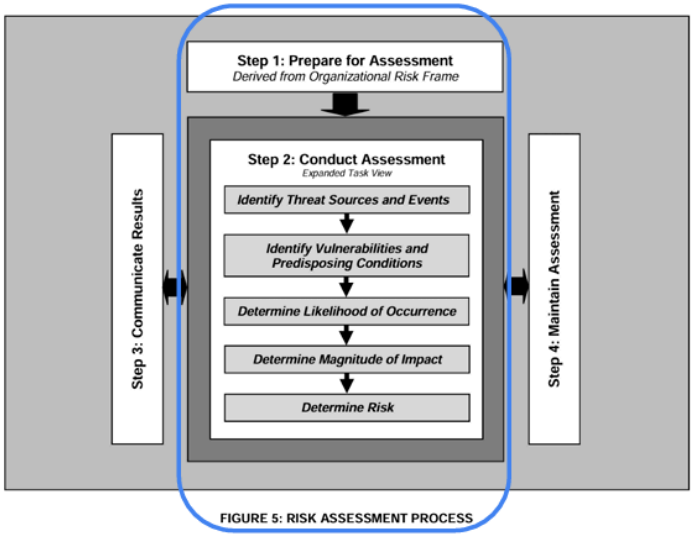

FIGURE 5: RISK ASSESSMENT PROCESS

Ipotizzate che l'organizzazione può accettare solamente un rischio basso per tutti gli eventi di rischio identificati, dovuto al valore del loro asset principale «dati sanitari». Fate delle valutazioni e delle ipotesi sui prossimi passaggi da eseguire per riportare il livello di rischio ottenuto entro quello desiderato.

https://csrc.nist.gov/pubs/sp/800/30/r1/final

Identificazione dello scenario

L'azienda Alpha è un fornitore leader di servizi sanitari online che gestisce un'ampia infrastruttura IT che include sistemi basati su cloud, applicazioni web e dispositivi mobili. L'azienda gestisce anche dati sanitari sensibili per i propri pazienti.

- L'organizzazione si è resa conto di essere target di un gruppo criminale organizzato con un buon livello di preparazione e delle significative risorse per condurre attacchi coordinati.

Dai sistemi di monitoraggio, è emerso che solo questa azienda è continuamente sorvegliata dal gruppo criminale. Da ulteriori analisi, si arriva alla conclusione che il gruppo criminale vuole esfiltrare delle informazioni all'azienda sui dati sanitari degli utenti per rivenderli, creando una persistenza all'interno dell'organizzazione e non facendosi rilevare.

- In questo momento la sorgente delle minacce è alla fase di ricognizione esterna con diversi metodi (scanning, sniffing, OSINT, sorveglianza), non si rilevano ricognizioni interne
- L'organizzazione non ha abilitato MFA e non effettua regolarmente Vulnerability Assessment
- L'organizzazione tratta informazioni personali e il loro software deve consentire la condivisione delle informazioni tra gli utenti, ciò si applica alla maggior parte dei loro sistemi.
- Tutte le attività di ricognizioni sono attive, però lo scanning e sniffing portano a degli impatti bassi perché presente un firewall e WAF su cloud, invece gli effetti potrebbero essere moderati nella ricerca open source o nella sorveglianza di alcuni target particolari.

1. Prepare for Assessment

1.1 Scopo del risk assessment:

1. Identificare e valutare i rischi associati alla sicurezza delle informazioni e alla protezione dei dati sanitari sensibili dell'azienda Alpha.
2. Valutare il livello di esposizione dell'azienda ai potenziali attacchi e alle minacce provenienti dal gruppo criminale organizzato.
3. Identificare le vulnerabilità presenti nei sistemi e nelle procedure dell'azienda che potrebbero essere sfruttate dai criminali per esfiltrare i dati dei pazienti.

1.2 Ambito del risk assessment:

1. L 'ambito include la sicurezza delle informazioni e la protezione dei dati sanitari gestiti dall'azienda Alpha.
2. Si concentra sull'analisi delle minacce esterne provenienti dal gruppo criminale organizzato e sulle vulnerabilità presenti nei sistemi IT dell'azienda.

1.3 Ipotesi e vincoli del risk assessment:

1. **Ipotesi**:
    a. Il gruppo criminale organizzato ha una buona preparazione e risorse significative per condurre attacchi mirati.
    b. L'obiettivo del gruppo criminale è esfiltrare informazioni sui dati sanitari degli utenti dell'azienda per rivenderli.

c. Il gruppo criminale desidera mantenere una persistenza all'interno dell'organizzazione senza essere rilevato.

2. **Vincoli**:

   a. L'organizzazione non ha abilitato l'autenticazione multi-fattore (MFA) e non effettua regolarmente la valutazione delle vulnerabilità (Vulnerability Assessment).

   b. I sistemi software dell'organizzazione devono consentire la condivisione delle informazioni tra gli utenti, rendendo necessaria una valutazione aggiuntiva dei rischi associati a questa funzionalità.

1.4 Sorgenti di informazioni per threat, vulnerabilità e impatti:

1. Sorgenti di informazioni per le minacce (threat sources): gruppi criminali organizzati, hacker, attaccanti esterni con intenti malevoli.
2. Sorgenti di informazioni per le vulnerabilità: analisi delle configurazioni dei sistemi IT dell'azienda, informazioni pubbliche su vulnerabilità note nei software utilizzati dall'azienda.
3. Sorgenti di informazioni per gli impatti: analisi delle conseguenze potenziali di un'eventuale violazione dei dati sanitari dei pazienti, inclusi impatti finanziari, reputazionali e legali.

2. Conduct Assessment

2.1 Identify threat sources - Appendice D

Questo allegato fornisce:

I. una descrizione di input potenzialmente utili per l'identificazione delle fonti di minaccia;
II. una tassonomia esemplificativa delle fonti di minaccia per tipo, descrizione e fattori di rischio (ossia, caratteristiche) utilizzati per valutare la probabilità e/o l'impatto di tali fonti di minaccia nell'iniziare eventi di minaccia;
III. un insieme esemplificativo di scale di valutazione adattabili per valutare quei fattori di rischio; e
IV. modelli per riassumere e documentare i risultati del Task 2-1 di identificazione delle fonti di minaccia.

La tassonomia e le scale di valutazione in questo allegato possono essere utilizzate dalle organizzazioni come punto di partenza con una personalizzazione appropriata per adattarsi alle condizioni specifiche dell'organizzazione. Le tabelle D-7 e D-8, risultati del Task 2-1, forniscono input rilevanti alle tabelle di rischio nell'Allegato I.

TABLE D-7: TEMPLATE – IDENTIFICATION OF ADVERSARIAL THREAT SOURCES

Identifier	Threat Source Source of Information	In Scope	Capability	Intent	Targeting
Organization -defined	Table D-2 and Task 1-4 or Organization-defined	Yes / No	Table D-3 or Organization -defined	Table D-4 or Organization -defined	Table D-5 or Organization -defined

TABLE D-7: IDENTIFICATION OF ADVERSARIAL THREAT SOURCES					
Minaccia	**Threat source**	**In Scope**	**Capability**	**Intent**	**Targeting**
Attacco informatico	Un attaccante compromette la sicurezza dei server aziendali attraverso vulnerabilità software o tecniche di phishing	Si	Alta: L'avversario ha un livello sofisticato di competenza, con risorse e opportunità significative per supportare più attacchi coordinati di successo.	Medio: L'avversario cerca di ottenere o modificare specifiche informazioni critiche o sensibili o di usurpare/interrompere le risorse informatiche dell'organizzazione stabilendo un punto d'appoggio nei sistemi informativi o nell'infrastruttura dell'organizzazione.	Alto: L'avversario analizza le informazioni ottenute tramite ricognizione per prendere di mira in modo persistente una specifica organizzazione, impresa, programma, missione o funzione aziendale, concentrandosi su specifiche informazioni, risorse, flussi di fornitura o funzioni di alto valore o mission-critical, dipendenti specifici che supportano tali funzioni, o posizioni chiave.
ACCIDENTALE - Utente - Utente/Amministratore privilegiato	Azioni errate intraprese da individui nel corso dell'esecuzione delle loro responsabilità quotidiane.	Si	Alta: L'avversario sfruttando tecniche OSINT può approfittare delle "debolezze" degli utenti	Medio: L'avversario cerca di ottenere o modificare specifiche informazioni critiche o sensibili o di usurpare/interrompere risorse informatiche dell'organizzazione	Medio: L'avversario analizza le informazioni disponibili al pubblico per prendere di mira in modo persistente specifici valori organizzativi

2.2 Identify threat events - Appendice E

Questo allegato fornisce:

I. una descrizione di potenziali input utili per l'identificazione degli eventi minacciosi;
II. esempi rappresentativi di eventi minacciosi avversari espressi come tattiche, tecniche e procedure (TTP) e eventi minacciosi non avversari;
III. una scala di valutazione esemplificativa per la rilevanza di tali eventi minacciosi; e

IV. modelli per riassumere e documentare i risultati del Task 2-2 di identificazione delle minacce.

Le organizzazioni possono eliminare certi eventi minacciosi dalla considerazione ulteriore se non è stato identificato alcun avversario con la capacità necessaria. Le organizzazioni possono anche modificare gli eventi minacciosi forniti per descrivere specifiche TTP con sufficiente dettaglio e al livello di classificazione appropriato. Le organizzazioni possono utilizzare gli eventi minacciosi rappresentativi e i valori predetti/previsti per la rilevanza di quegli eventi come punto di partenza, adattandoli per adattarsi a eventuali condizioni specifiche dell'organizzazione. La Tabella E-5, un output dal Task 2-2, fornisce input rilevanti per le tabelle di rischio nell'Allegato I.

TABLE E-5: TEMPLATE – IDENTIFICATION OF THREAT EVENTS

Identifier	Threat Event Source of Information	Threat Source	Relevance
Organization-defined	Table E-2, Table E-3, Task 1-4 or Organization-defined	Table D-7, Table D-8 or Organization-defined	Table E-4 or Organization-defined

TABELLA E-5: IDENTIFICAZIONE DEGLI EVENTI DI MINACCIA			
Minaccia	**Threat event**	**Threat Source**	**Relevance**
Adattare gli attacchi informatici basandosi su una sorveglianza dettagliata	L'avversario adatta il comportamento in risposta alla sorveglianza e alle misure di sicurezza organizzative.		Confermato: L'evento di minaccia o TTP è stato rilevato dall'organizzazione

Offuscare le azioni dell'avversario.	L'avversario intraprende azioni per inibire l'efficacia dei sistemi di rilevamento delle intrusioni o delle capacità di controllo all'interno delle organizzazioni.	Un attaccante compromette la sicurezza dei dati dei pazienti attraverso vulnerabilità software o tecniche di phishing	Previsto: L'evento di minaccia o TTP è stato previsto da una fonte attendibile.
Adattare gli attacchi informatici basandosi su una sorveglianza dettagliata.	L'avversario adatta il comportamento in risposta alla sorveglianza e alle misure di sicurezza organizzative.		
Ottenere dati/informazioni sensibili da sistemi informativi accessibili al pubblico.	L'avversario scansiona o estrae informazioni su server e pagine Web di organizzazioni accessibili pubblicamente con l'intento di trovare informazioni sensibili.		Confermato: L'evento di minaccia o TTP è stato rilevato dall'organizzazione
Causare la divulgazione non autorizzata e/o l'indisponibilità divulgando informazioni sensibili.	L'avversario contamina i sistemi informativi organizzativi (inclusi dispositivi e reti) inducendoli a gestire informazioni di una classificazione/sensibilità per la quale non sono stati autorizzati. Le informazioni vengono esposte a individui non autorizzati ad accedervi e il sistema informativo, il dispositivo o la rete non sono disponibili mentre la fuoriuscita viene indagata e mitigata.		Possibile: L'evento di minaccia o TTP è stato descritto da una fonte alquanto credibile.
Insider threat	I dipendenti dell'azienda potrebbero rappresentare una minaccia interna se agiscono in modo malevolo o se commettono errori non intenzionali	La divulgazione non autorizzata di informazioni sensibili	Possibile: L'evento di minaccia o TTP è stato descritto da una fonte alquanto credibile.

2.3 Identify vulnerabilities and predisposing conditions - Appendice F

Questo allegato fornisce:

I. una descrizione di potenziali input utili per l'identificazione delle vulnerabilità e delle condizioni predisponenti;

II. una tassonomia esemplificativa delle condizioni predisponenti;
III. scale di valutazione esemplificative per valutare la gravità delle vulnerabilità e la pervasività delle condizioni predisponenti; e
IV. un insieme di modelli per riassumere e documentare i risultati dell'attività di identificazione delle vulnerabilità e delle condizioni predisponenti.

La tassonomia e le scale di valutazione in questo allegato possono essere utilizzate dalle organizzazioni come punto di partenza con l'adeguata personalizzazione per adattarsi a eventuali condizioni specifiche dell'organizzazione. Le Tabelle F-3 e F-6, output dalla Task 2-3, forniscono input rilevanti alle tabelle del rischio nell'Allegato I.

TABLE F-3: TEMPLATE – IDENTIFICATION OF VULNERABILITIES

Identifier	Vulnerability Source of Information	Vulnerability Severity
Organization-defined	Task 2-3, Task 1-4 or Organization-defined	Table F-2 or Organization-defined

TABELLA F-3: IDENTIFICAZIONE DELLE VULNERABILITA’		
Minaccia	**Vulnerabilità**	**Gravità delle vulnerabilità**
Mancanza di aggiornamenti regolari	La versione attuale dell’applicazione non gestisce correttamente le credenziali di accesso.	Alta: La vulnerabilità è estremamente preoccupante, in base all'esposizione della vulnerabilità e alla facilità di sfruttamento e/o alla gravità degli impatti che potrebbero derivare dal suo sfruttamento. Sono pianificati ma non implementati i relativi controlli di sicurezza o altri interventi correttivi; i controlli compensativi sono in atto e sono almeno minimamente efficaci.
Violazioni della sicurezza dei dispositivi mobili	I dispositivi potrebbero essere vulnerabili a perdite di dati o accessi non autorizzati se non sono adeguatamente protetti da misure di sicurezza, come l'uso di app di messaggistica sicura o la crittografia dei dati.	Alta: La vulnerabilità è estremamente preoccupante, in base all'esposizione della vulnerabilità e alla facilità di sfruttamento e/o alla gravità degli impatti che potrebbero derivare dal suo sfruttamento. Sono pianificati ma non implementati i relativi controlli di sicurezza o altri interventi correttivi; i controlli compensativi sono in atto e sono almeno minimamente efficaci.

Attacchi informatici	L'azienda potrebbe essere soggetta a attacchi informatici mirati come phishing, malware, attacchi DDoS, hacking o exploit delle vulnerabilità software, che potrebbero compromettere la disponibilità, l'integrità o la riservatezza dei dati.	Media: La vulnerabilità è di moderata preoccupazione, in base all'esposizione della vulnerabilità e alla facilità di sfruttamento e/o alla gravità degli impatti che potrebbero derivare dal suo sfruttamento. Il controllo di sicurezza pertinente o altre soluzioni correttive sono parzialmente implementati e in qualche modo efficaci.
Vulnerabilità delle applicazioni web e dei sistemi basati su cloud	Le applicazioni web e i sistemi cloud possono essere esposti a vulnerabilità software come bug o falle di sicurezza, che potrebbero essere sfruttate da hacker per accedere ai dati sensibili dei pazienti.	Media: La vulnerabilità è di moderata preoccupazione, in base all'esposizione della vulnerabilità e alla facilità di sfruttamento e/o alla gravità degli impatti che potrebbero derivare dal suo sfruttamento. Il controllo di sicurezza pertinente o altre soluzioni correttive sono parzialmente implementati e in qualche modo efficaci.
Accessi non autorizzati violazioni della privacy	Potrebbero verificarsi accessi non autorizzati ai dati dei pazienti a causa di debolezze nella gestione degli accessi o della mancanza di controlli di sicurezza adeguati, mettendo a rischio la privacy e la riservatezza delle informazioni sanitarie	Media: La vulnerabilità è di moderata preoccupazione, in base all'esposizione della vulnerabilità e alla facilità di sfruttamento e/o alla gravità degli impatti che potrebbero derivare dal suo sfruttamento. Il controllo di sicurezza pertinente o altre soluzioni correttive sono parzialmente implementati e in qualche modo efficaci.

TABLE F-6: TEMPLATE – IDENTIFICATION OF PREDISPOSING CONDITIONS

Identifier	Predisposing Condition Source of Information	Pervasiveness of Condition
Organization-defined	Table F-4, Task 1-4 or Organization-defined	Table F-5 or Organization-defined

TABELLA F-6: IDENTIFICAZIONE DELLE CONDIZIONI PREDISPOSTE		
Minaccia	**Condizione di predisposizione**	**Pervasività* della condizione (*Diffusione/estensione)**
Mancanza di aggiornamenti regolari	Informazioni di identificazione personale: Ha bisogno di utilizzare le tecnologie in modi specifici.	Alta: Si applica alla maggior parte delle missioni organizzative/funzioni aziendali (Tier 1), missione/processi aziendali (Tier 2) o sistemi informativi (Tier 3).
Violazioni della sicurezza dei dispositivi mobili	Ha bisogno di utilizzare le tecnologie in modi specifici.	Bassa: Si applica ad alcune delle missioni organizzative/funzioni aziendali (Tier 1), missione/processi aziendali (Tier 2) o sistemi informativi (Tier 3).
Attacchi informatici	Programmi di accesso speciale	Alta: Si applica alla maggior parte delle missioni organizzative/funzioni aziendali (Tier 1), missione/processi aziendali (Tier 2) o sistemi informativi (Tier 3).
Vulnerabilità delle applicazioni web e dei sistemi basati su cloud	Determinato dall'accordo con il gestore del cloud	Bassa: Si applica ad alcune delle missioni organizzative/funzioni aziendali (Tier 1), missione/processi aziendali (Tier 2) o sistemi informativi (Tier 3).
Accessi non autorizzati violazioni della privacy	Informazioni di identificazione personale	Alta: Si applica alla maggior parte delle missioni organizzative/funzioni aziendali (Tier 1), missione/processi aziendali (Tier 2) o sistemi informativi (Tier 3).
Minaccia interna	Errore umano nel aprire link malevoli	Bassa: Si applica ad alcune delle missioni organizzative/funzioni aziendali (Tier 1), missione/processi aziendali (Tier 2) o sistemi informativi (Tier 3).

2.4 Determine likelihood - Appendice G

Questo allegato fornisce:

I. una descrizione di input potenzialmente utili per la determinazione della probabilità; e
II. esempi di scale di valutazione per valutare la probabilità dell'inizio/verificarsi di eventi minacciosi, la probabilità che gli eventi minacciosi producano impatti negativi e la probabilità complessiva che gli eventi minacciosi vengano iniziati o verificati e causino danni alle operazioni, agli asset o alle persone dell'organizzazione.

Le scale di valutazione in questo allegato possono essere utilizzate dalle organizzazioni come punto di partenza con una personalizzazione appropriata per adattarsi a eventuali condizioni specifiche dell'organizzazione. Le tabelle G-2, G-3, G-4 e G-5, output da Task 2-4, forniscono input rilevanti alle tabelle di rischio nell'Allegato I.

TABLE G-5: ASSESSMENT SCALE – OVERALL LIKELIHOOD

Likelihood of Threat Event Initiation or Occurrence	Likelihood Threat Events Result in Adverse Impacts				
	Very Low	Low	Moderate	High	Very High
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

2.5 Determine Impact - Appendice H

Questa appendice fornisce:

I. una descrizione di input utili per il compito di determinazione dell'impatto;
II. esempi rappresentativi di impatti negativi sulle operazioni e gli asset organizzativi, sugli individui, su altre organizzazioni o sulla Nazione;

III. scale di valutazione esemplificative per valutare l'impatto degli eventi minacciosi e la gamma di effetti degli eventi minacciosi; e

IV. un modello per riassumere e documentare i risultati del compito di determinazione dell'impatto 2-5.

Le scale di valutazione in questa appendice possono essere utilizzate come punto di partenza con la personalizzazione appropriata per adattarsi a eventuali condizioni specifiche dell'organizzazione. La Tabella H-4, un output del compito 2-5, fornisce input rilevanti per le tabelle dei rischi nell'Appendice I.

TABLE H-4: TEMPLATE – IDENTIFICATION OF ADVERSE IMPACTS

Type of Impact	Impact Affected Asset	Maximum Impact
Table H-2 or Organization-defined	Table H-2 or Organization-defined	Table H-3 or Organization-defined

TABELLA H-4: IDENTIFICAZIONE DEGLI IMPATTI NEGATIVI		
Tipo di impatto	**Impatto Asset interessati**	**Impatto massimo**
Danno alle operazioni	Incapacità di svolgere missioni/funzioni aziendali attuali. - In modo sufficientemente tempestivo. - Con sufficiente sicurezza e/o correttezza. - Entro i limiti delle risorse pianificate. Furto d'identità e perdita di informazioni di identificazione personale.	Medio: Si potrebbe prevedere che l'evento di minaccia abbia un grave effetto negativo sulle operazioni organizzative, sui beni organizzativi, sugli individui, su altre organizzazioni o sulla Nazione. Un effetto avverso grave significa che, ad esempio, l'evento di minaccia potrebbe: (i) causare un significativo degrado della capacità della missione in una misura e una durata tali da consentire all'organizzazione di svolgere le sue funzioni primarie, ma l'efficacia delle funzioni è significativamente ridotta ; (ii) comportare
Danno agli individui		

Danno alle operazioni	- Incapacità, o capacità limitata, di svolgere missioni con sufficiente sicurezza e/o correttezza. - Danni (ad esempio, costi finanziari, sanzioni) dovuti alla non conformità. - Danni relazionali. - Danni ai rapporti fiduciari. - Danno all'immagine o alla reputazione (e quindi ai futuri o potenziali rapporti fiduciari)	danni significativi al patrimonio organizzativo; (iii) comportare perdite finanziarie significative; o (iv) provocare danni significativi a individui che non comportino la perdita della vita o lesioni gravi mortali.
Danni ad altre organizzazioni	Danni alla reputazione e ai rapporti fiduciari	

2.6 Determine Risk - Appendice I

Questo allegato fornisce:

I. una descrizione dei potenziali input utili per il compito di determinazione del rischio, inclusi considerazioni per l'incertezza delle determinazioni;
II. scale di valutazione esemplificative per valutare i livelli di rischio;
III. tabelle per descrivere il contenuto (cioè, input di dati) per le determinazioni di rischio avversarie e non avversarie; e
IV. modelli per riassumere e documentare i risultati del compito di determinazione del rischio 2-6.
V. Le scale di valutazione in questo allegato possono essere utilizzate come punto di partenza con una personalizzazione appropriata per adattarsi a eventuali condizioni specifiche dell'organizzazione. La Tabella I-5 (rischio avversario) e la Tabella I-7 (rischio non avversario) sono risultati dal Compito 2-6.

TABLE I-5: TEMPLATE – ADVERSARIAL RISK

1	2	3	4	5	6	7	8	9	10	11	12	13
Threat Event	Threat Sources	Threat Source Characteristics			Relevance	Likelihood of Attack Initiation	Vulnerabilities and Predisposing Conditions	Severity and Pervasiveness	Likelihood Initiated Attack Succeeds	Overall Likelihood	Level of Impact	Risk
		Capability	Intent	Targeting								

TABELLA I-5: RISCHIO CONTROVERSO												
1	2	3	4	5	6	7	8	9	10	11	12	13
Treat event	Threat source	Threat source Characteristics			Relevance	Likleihood of attack initiation	Vulnerabilities and predisposing conditions	Likelihood Initialited Attack Successeds	Severity and pervasiveness	Overall likelihood (G-5)	Level of Impact	Risk (I-2)
		Capability	Intent	Targeting								
L'avversario contamina i sistemi informativi organizzativi (inclusi dispositivi e reti) inducendoli a gestire informazioni di una classificazione/sensibilità per la quale non sono stati autorizzati. Le informazioni vengono esposte a individui non autorizzati ad accedervi e il sistema informativo, il dispositivo o la rete non sono disponibili mentre la fuoriuscita viene indagata e mitigata.	Un attaccante compromette la sicurezza dei server aziendali attraverso vulnerabilità software o tecniche di phishing	Alto	Medio	Alto	Possibile	Medio	Informazioni di identificazione personale	Alto	Molto alto	Alto	Alto	Medio
I dipendenti dell'azienda potrebbero rappresentare una minaccia interna se agiscono in modo malevolo o se commettono errori non intenzionali	La divulgazione non autorizzata di informazioni sensibili	Alto	Medio	Medio	Possibile	Basso	Errore umano nel aprire link malevoli	Alto	Molto alto	Alto	Alto	Medio

TABELLA I-5: RISCHIO CONTROVERSO												
1	2	3	4	5	6	7	8	9	10	11	12	13
Treat event	Threat source	Threat source Characteristics			Relevance	Likleihood of attack initiation	Vulnerabilities and predisposing conditions	Likelihood Initialited Attack Successeds	Severity and pervasiveness	Overall likelihood (G-5)	Level of Impact	Risk (I-2)
		Capability	Intent	Targeting								
L'avversario adatta il comportamento in risposta alla sorveglianza e alle misure di sicurezza organizzative.	Un attaccante compromette la sicurezza dei server aziendali attraverso vulnerabilità software o tecniche di phishing	Alto	Medio	Alto	Confermato	Alto	Informazioni di identificazione personale: Ha bisogno di utilizzare le tecnologie in modi specifici.	Alto	Molto alto	Alto	Alto	Medio
L'avversario intraprende azioni per inibire l'efficacia dei sistemi di rilevamento delle intrusioni o delle capacità di controllo all'interno delle organizzazioni.		Alto	Medio	Alto	Previsto	Medio	Ha bisogno di utilizzare le tecnologie in modi specifici.	Alto	Molto alto	Alto	Alto	Medio
L'avversario adatta il comportamento in risposta alla sorveglianza e alle misure di sicurezza organizzative.		Alto	Medio	Alto	Previsto	Medio	Programmi di accesso speciale	Alto	Molto alto	Alto	Alto	Medio
L'avversario scansiona o estrae informazioni su server e pagine Web di organizzazioni accessibili pubblicamente con l'intento di trovare informazioni sensibili.	Un attaccante compromette la sicurezza dei server aziendali attraverso vulnerabilità software o tecniche di phishing	Alto	Medio	Alto	Confermato	Molto alto	Determinato dall'accordo con il gestore del cloud	Alto	Molto alto	Alto	Alto	Medio

3. Comunicazione dei risultati

Conclusione del Report di Risk Assessment:

In conclusione, il risk assessment condotto sull'azienda Alpha, un fornitore leader di servizi sanitari online, ha rilevato un grado di rischio medio associato alla gestione di un'ampia infrastruttura IT che comprende sistemi basati su cloud, applicazioni web e dispositivi mobili, oltre alla gestione di dati sanitari sensibili per i pazienti. Tuttavia, è importante notare che il grado di rischio accettato dall'azienda è basso, indicando un impegno adeguato verso la sicurezza delle informazioni e la protezione dei dati sensibili.

Nonostante il basso grado di rischio accettato, è chiaro che alcune vulnerabilità e minacce persistono e richiedono azioni di mitigazione mirate. Queste operazioni di mitigazione dovrebbero essere progettate e implementate con cura per ridurre ulteriormente il rischio e rafforzare la sicurezza complessiva dell'azienda. Le specifiche azioni di mitigazione verranno discusse in dettaglio nel piano di azione successivo, che delineerà le misure specifiche da adottare per affrontare le vulnerabilità identificate e migliorare la posizione di sicurezza dell'azienda.

L'azienda Alpha è ben posizionata per affrontare le sfide relative alla sicurezza delle informazioni, ma è fondamentale perseguire un approccio proattivo per garantire la protezione continua dei dati dei pazienti e la sicurezza delle operazioni aziendali.

4. Operazioni di mitigazioni consigliate

Autenticazione e controllo degli accessi:

1.
2. **Implementazione dell'autenticazione multi-fattore (MFA):** L'abilitazione di MFA aggiunge un livello aggiuntivo di sicurezza, rendendo più difficile per gli attaccanti ottenere l'accesso non autorizzato. Questo può ridurre significativamente il rischio di compromissione dell'account.
3. **Implementazione di controlli di accesso basati sui ruoli:** Definire e applicare restrizioni di accesso basate sui ruoli dei dipendenti può garantire che solo coloro che hanno effettivamente bisogno di accedere ai dati sensibili siano in grado di farlo.
4. **Adozione di una strategia di Zero Trust**: Rivedere e aggiornare l'approccio di sicurezza per adottare un modello Zero Trust, in cui ogni richiesta di accesso è considerata non affidabile fino a prova contraria. Ciò può essere realizzato tramite l'implementazione di controlli di accesso granulari e l'uso di tecniche come la micro segmentazione della rete.
5. **Limitazione dell'accesso ai dati sensibili**: Ridurre al minimo l'accesso ai dati sensibili solo al personale autorizzato può limitare l'esposizione dei dati e ridurre il rischio di compromissione.

Vulnerabilità del sistema e patching:

6. **Condurre regolarmente valutazioni delle vulnerabilità**: L'organizzazione dovrebbe iniziare a eseguire regolarmente valutazioni delle vulnerabilità per identificare e correggere potenziali falle di sicurezza nei propri sistemi. Questo può aiutare a mitigare il rischio di exploit da parte degli attaccanti.
7. **Aggiornamento e patching regolare dei sistemi e delle applicazioni**: Mantenere i sistemi e le applicazioni aggiornati con le ultime patch di sicurezza può aiutare a proteggere da vulnerabilità note e a ridurre il rischio di exploit.

8. **Monitoraggio dell'Open Source Intelligence (OSINT) per identificare potenziali minacce:** Tenere traccia delle informazioni disponibili pubblicamente su internet può aiutare a identificare potenziali minacce e a mitigare i rischi in modo proattivo.

Sicurezza del cloud e protezione dei dati:

9. **Rafforzamento delle misure di sicurezza del cloud**: Poiché l'azienda utilizza un'infrastruttura basata su cloud, è essenziale implementare misure di sicurezza robuste come firewall e Web Application Firewall (WAF) per proteggere i dati sensibili dai tentativi di accesso non autorizzato.
10. **Criptazione dei dati sensibili durante il trasferimento e l'archiviazione**: Utilizzare la crittografia per proteggere i dati sensibili durante il trasferimento e l'archiviazione può renderli inutilizzabili per gli attaccanti anche se riescono ad accedervi.
11. **Valutazione e mitigazione dei rischi dei fornitori:** Verificare e valutare la sicurezza dei fornitori di servizi e terze parti con accesso ai dati sensibili può contribuire a proteggere l'azienda da possibili punti di ingresso per gli attaccanti.

Rilevamento delle minacce e risposta agli incidenti:

12. **Investimento in Threat Intelligence e monitoraggio delle minacce**: Investire in strumenti e tecnologie di monitoraggio delle minacce può aiutare a identificare e rispondere prontamente a comportamenti sospetti o attività anomale sulla rete. In questo modo, è possibile rilevare e rispondere agli attacchi in modo tempestivo.
13. **Implementazione di una soluzione di Deception Technology**: Utilizzare tecnologie di inganno per creare falsi punti di accesso e dati allettanti per gli attaccanti. Questo può aiutare a identificare e intrappolare gli aggressori, consentendo nel contempo all'organizzazione di monitorare le attività di ricognizione e di rispondere in modo proattivo agli attacchi.
14. **Adottare una soluzione di Gestione delle minacce endpoint (EDR):** Utilizzare una soluzione di EDR per rilevare, analizzare e rispondere agli attacchi avanzati sui dispositivi endpoint, proteggendo così i dati sanitari degli utenti che potrebbero essere accessibili tramite tali dispositivi.

15. **Integrare l'intelligenza artificiale e l'apprendimento automatico per la sicurezza**: Utilizzare strumenti avanzati basati sull'intelligenza artificiale e sull'apprendimento automatico per analizzare i modelli di traffico e identificare comportamenti anomali che potrebbero indicare attività sospette o attacchi in corso
16. **Aumentare la consapevolezza della sicurezza:** È importante sensibilizzare tutti i dipendenti sull'importanza della sicurezza informatica e sulle pratiche migliori. Questo può essere fatto attraverso la formazione e l'educazione sui rischi informatici e sulle tecniche di attacco più comuni.

Protezione dalle minacce e-mail:

17. **Implementare controlli di protezione avanzati per la posta elettronica:** Utilizzare soluzioni avanzate di filtraggio delle email e di protezione dalle frodi per proteggere dagli attacchi di phishing e di spoofing, che potrebbero essere utilizzati dal gruppo criminale per ottenere accesso non autorizzato ai dati.

Preparazione finanziaria:

18. **Sottoscrivere un'assicurazione contro le violazioni dei dati:** Considerare l'acquisto di un'assicurazione contro le violazioni dei dati per coprire i potenziali costi finanziari derivanti da una violazione della sicurezza, come le spese legali e i risarcimenti ai pazienti colpiti.

Struttura della rete e segmentazione:

19. **Segmentazione della rete**: Suddividere la rete aziendale in segmenti separati e applicare rigorose politiche di accesso può aiutare a limitare la diffusione di un eventuale attacco e a proteggere i dati sensibili.

5. Conclusioni

Quando si affronta la questione della sicurezza e delle mitigazioni proposte, è essenziale condurre un'analisi completa dei costi coinvolti. Questo processo implica l'identificazione e la valutazione di tutti i costi associati all'implementazione delle misure di sicurezza. Dalla progettazione e implementazione delle soluzioni tecniche alla formazione del personale e alla gestione continua della sicurezza, ogni aspetto finanziario deve essere preso in considerazione.

Una parte fondamentale di questo processo è l'analisi costi-benefici. Questo implica la valutazione degli investimenti necessari per implementare le misure di sicurezza proposte e la stima dei benefici che deriverebbero da queste misure in termini di riduzione del rischio e delle perdite potenziali. È qui che emerge il principio della Gordon-Loeb, che stabilisce un limite massimo ragionevole per gli investimenti in sicurezza in relazione alle perdite potenziali. Questo limite del 37% delle perdite potenziali fornisce un punto di riferimento utile per valutare se gli investimenti proposti sono proporzionati al rischio mitigato.

Inoltre, è importante considerare l'analisi del Return on Security Investment (ROSI) e del Return on Investment (ROI). Il ROSI misura l'efficacia degli investimenti in sicurezza confrontando i benefici ottenuti con i costi sostenuti per ottenere tali benefici. Il ROI, d'altra parte, valuta il rendimento degli investimenti in sicurezza confrontando i guadagni ottenuti (o le perdite evitate) con i costi totali dell'investimento. Questi indicatori forniscono una visione chiara della fattibilità finanziaria del piano di sicurezza proposto e aiutano a prendere decisioni informate sulle priorità di investimento.

Un approccio che include un'analisi dettagliata dei costi, una valutazione costi-benefici e la misurazione del ROSI e del ROI è fondamentale per determinare la fattibilità e l'efficacia di un piano di sicurezza proposto.

Questo processo garantisce che gli investimenti in sicurezza siano proporzionati al rischio mitigato e che portino a risultati tangibili e sostenibili per l'organizzazione.