PHANTOM SRL

RISK ASSESSMENT

REPORT

Presented By : Iannone Luca
Pignatello Giuseppe
D'Ottavio Alessio

8 May 2024

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

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.

INFORMAZIONI NIST:

HTTPS://CSRC.NIST.GOV/PUBS/SP/800/30/R1/FINAL

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.

PASSAGGIO 1:
PREPARARSI PER LA VALUTAZIONE

Definire l'ambito e gli obiettivi della valutazione del rischio:
L'obiettivo principale è valutare i rischi associati alle minacce relative alle informazioni sistemiche di livello Tier 3 nell'azienda Alpha, con particolare attenzione alla possibile esfiltrazione di dati sanitari sensibili da parte di un gruppo criminale organizzato.

Raccolta delle informazioni di contesto:
Raccogliamo informazioni dettagliate sull'infrastruttura IT dell'azienda Alpha, inclusi i sistemi basati su cloud, le applicazioni web, i dispositivi mobili e i dati sanitari sensibili gestiti.

Identificazione delle fonti di minaccia specifiche per Tier 3: Basandoci sulla mappa delle relazioni tra tabelle, identifichiamo le principali fonti di minaccia specifiche per Tier 3 nell'ambito dell'azienda Alpha.

Queste includono il gruppo criminale organizzato, che mira all'esfiltrazione di dati sanitari sensibili per motivi di lucro.

Analisi delle vulnerabilità esistenti:
Esaminiamo le vulnerabilità presenti nei sistemi IT dell'azienda Alpha.
In particolare, notiamo che l'assenza di autenticazione a più fattori (MFA) e la mancanza di esecuzione regolare di valutazioni delle vulnerabilità possono aumentare il rischio di compromissione dei dati(alessio d’ottavio ricchio).

PASSAGGIO 2: CONDURRE LA VALUTAZIONE

Identificare i possibili scenari di minaccia: Basandoci sulle informazioni raccolte, identifichiamo possibili scenari di minaccia. Ad esempio, uno scenario potrebbe coinvolgere un attacco di **phishing** mirato per ottenere credenziali di accesso a sistemi sensibili.

Valutare l'impatto potenziale: Consideriamo gli impatti potenziali dei vari scenari di minaccia sull'azienda Alpha. Ad esempio, l'esfiltrazione di dati sanitari sensibili potrebbe causare danni finanziari, danneggiare la reputazione dell'azienda e violare le normative sulla privacy dei dati.

Determinare la probabilità di accadimento: Valutiamo la probabilità che ciascuno scenario di minaccia si verifichi, tenendo conto delle misure di sicurezza attualmente implementate e delle capacità del gruppo criminale organizzato. (Considerando le attuali difese dell'azienda, stimiamo che il 75 % degli attacchi non vadano a buon fine, vista la mancata esecuzione di VA e la mancanza di autenticazione a multi fattori).

Stimare il rischio: Utilizzando una combinazione di impatto potenziale e probabilità di accadimento, stimiamo il rischio associato a ciascuno scenario di minaccia identificato. Ad esempio, potremmo concludere che l'esfiltrazione di dati sanitari sensibili rappresenta un rischio significativo per l'azienda Alpha e richiede azioni correttive immediate.

Documentare i risultati: Documentiamo i risultati della valutazione del rischio, inclusi gli scenari di minaccia identificati, l'impatto potenziale e la probabilità di accadimento, insieme alle raccomandazioni per mitigare i rischi identificati.

Questa è una simulazione semplificata dei primi due passaggi di un processo di valutazione del rischio conforme al NIST SP 800-30, focalizzandoci sul Tier 3 dell'azienda Alpha.

ORIGINE DELLE MINACCE THREAT SOURCE (APPENDIX D)

Questo allegato fornisce: (i) una descrizione di input potenzialmente utili per l'attività di identificazione delle fonti di minaccia; (ii) una tassonomia esemplificativa delle fonti di minaccia per tipo, descrizione e fattori di rischio (cioè, caratteristiche) utilizzati per valutare la probabilità e/o l'impatto di tali fonti di minaccia nell'innesco di eventi di minaccia; (iii) un esemplare insieme di scale di valutazione adattabili per valutare quei fattori di rischio; e (iv) modelli per riassumere e documentare i risultati dell'attività di identificazione delle fonti di minaccia Task 2-1.
La tassonomia e le scale di valutazione in questo allegato possono essere utilizzate dalle organizzazioni come punto di partenza con un adattamento appropriato per adeguarsi a condizioni specifiche dell'organizzazione.
Le tabelle D-7 e D-8, output dalla 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.

EVENTI MINACCIOSI
THREAT EVENTS (APPENDIX E)

Questo allegato fornisce: (i) una descrizione di input potenzialmente utili per l'attività di identificazione degli eventi di minaccia; (ii) esempi rappresentativi di eventi di minaccia avversaria espressi come tattiche, tecniche e procedure (TTP) ed eventi di minaccia non avversari; (iii) una scala di valutazione esemplificativa per la rilevanza di quegli eventi di minaccia; e (iv) modelli per riassumere e documentare i risultati dell'attività di identificazione delle minacce Task 2-2.
Le organizzazioni possono eliminare certi eventi di minaccia dalla considerazione ulteriore se non è stato identificato nessun avversario con le capacità necessarie. Le organizzazioni possono anche modificare gli eventi di minaccia forniti per descrivere specifiche TTP con un dettaglio sufficiente e al livello di classificazione appropriato.
Le organizzazioni possono utilizzare gli eventi di minaccia rappresentativi e i valori previsti per la rilevanza di quegli eventi come punto di partenza con un adattamento per adeguarsi a eventuali condizioni specifiche dell'organizzazione. La tabella E-5, un output della Task 2-2, fornisce input rilevanti alle 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	Adattare gli attacchi informatici basandosi su una sorveglianza dettagliata	Un attaccante compromette la sicurezza dei dati dei pazienti attraverso	Confermato: L'evento di minaccia o TTP è stato rilevato dall'organizzazione

VULNERABILITÀ E CONDIZIONI PREDISPONENTI (APPENDIX 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 l'ampiamente delle condizioni predisponenti; e (iv) un insieme di modelli per riassumere e documentare i risultati dell'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 un adattamento appropriato per adeguarsi a eventuali condizioni specifiche dell'organizzazione.
Le tabelle F-3 e F-6, risultati della Task 2-3, forniscono input rilevanti per le tabelle di 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.

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 predisposta	Pervasività* della condizione (*Diffusione/estensione)
Mancanza di aggiornamenti regolari	Informazioni di identificazione personale: Ha bisogno di utilizzare le tecnologie in modi specifici.	Molto alta: Si applica a tutte le missioni organizzative/funzioni aziendali (Livello 1), missione/processi aziendali (Livello 2) o sistemi informativi (Livello 3).

EFFETTI DEGLI EVENTI MINACCIOSI (APPENDIX H)

Questo allegato fornisce: (i) una descrizione di input utili per l'attività 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 di minaccia e la gamma di effetti degli eventi di minaccia; e (iv) un modello per riassumere e documentare i risultati dell'attività di determinazione dell'impatto Task 2-5.
Le scale di valutazione in questo allegato possono essere utilizzate come punto di partenza con un adattamento appropriato per adeguarsi a eventuali condizioni specifiche dell'organizzazione.
La tabella H-4, un output dalla Task 2-5, fornisce input rilevanti alle tabelle di rischio nell'Allegato 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; Danno agli individui	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.	Moderato: 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 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.

RISCHIO AVVERSO
(APPENDIX 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

2	3	4	5	6	7	8	9	10	11	12	13
Threat source	Threat source Characteristics			Relevance	Likelihood 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								
Un attaccante compromette la sicurezza dei server aziendali attraverso vulnerabilità software o tecniche di phishing	Alta	Medio	Alto	Confermato	Alta	La versione attuale dell'applicazione non gestisce correttamente le credenziali di accesso.	Medio	Molto alta	Medio	Medio	Medio

ROSI:

SUPPONENDO DI AVERE I SEGUENTI DATI:
-ALE (PRIOR) €150,000
-ALE (POST) €75.000
- COSTO IMPLEMENTAZIONE DI SICUREZZA: €25.000

UTILIZZANDO QUESTI VALORI NELLA FORMULA DEL ROSI, OTTENIAMO:

ROSI = [(150,000 - 75.000)-25.000]/25.000

ROSI = 25.000/50.000

ROSI = 200%

QUINDI, IL ROSI È UGUALE AL 200%. CIO SIGNIFICA CHE L'INVESTIMENTO È CONVENIENTE PER L'AZIENDA.

GORDON LOEB:

PER CALCOLARE IL MODELLO DI GORDON-LOEB, UTILIZZIAMO LA FORMULA :

GORDON LOEB = 0.37 * D

DOVE "D" RAPPRESENTA IL VALORE MONETARIO EVITATO DELLE PERDITE GRAZIE AGLI INVESTIMENTI IN SICUREZZA.

CON I DATI FORNITI:

GORDON LOEB = 0.37 * €75.000

GORDON LOEB = €27.750

QUINDI, UTILIZZANDO I DATI FORNITI, IL VALORE DEL MODELLO DI GORDON-LOEB SAREBBE €27.750.

$$Investment = 0{,}37 \cdot d$$

$$d = \lambda \cdot t \cdot v$$

L'INVESTIMENTO QUINDI RISULTA CONVENIENTE SECONDO IL ROSI ED È IN LINEA CON IL MODELLO DI GORDON-LOEB.
L'INVESTIMENTO PERMETTERÀ ALL'AZIENDA DI AUMENTARE IL SUO MITIGATION RATIO IMPLEMENTANDO UN'AUTENTICAZIONE A MULTI FATTORI, ESEGUENDO 2 VULNERABILITY ASSESSMENT L'ANNO E FORMANDO I DIPENDENTI.

PHANTOM s.r.l
IMPOSSIBLE IS OUR TARGET

GRUPPO BCC
ICCREA

GRAZIE DELL'ATTENZIONE

08/05/2024

Prepared By:

GIUSEPPE PIGNATELLO
ALESSIO D'OTTAVIO
LUCA IANNONE

IANNONE LUCA
PIGNATELLO GIUSEPPE
D'OTTAVIO ALESSIO