RISK ASSESSMENT S2L5

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.

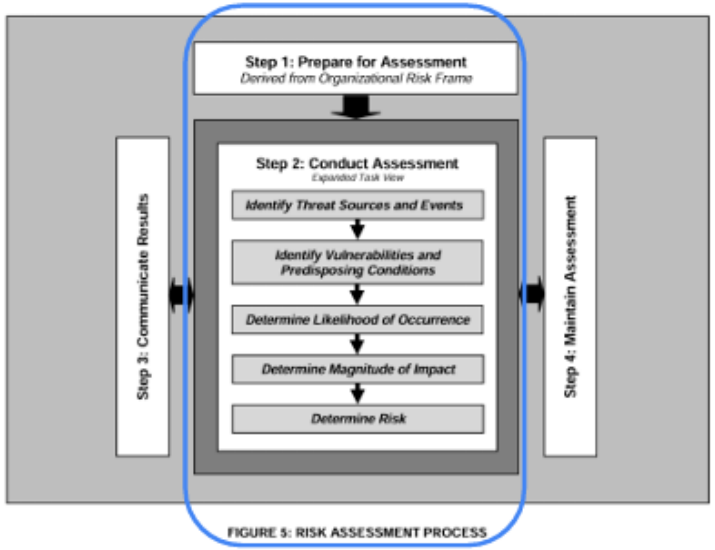

FIGURE 5: RISK ASSESSMENT PROCESS

TABLE D-1: INPUTS – THREAT SOURCE IDENTIFICATION

Description	Provided To		
	Tier 1	Tier 2	Tier 3

From Tier 1: (Organization level)
- Sources of threat information deemed to be credible (e.g., open source and/or classified threat reports, previous risk/threat assessments). (**Section 3.1, Task 1-4**)
- Threat source information and guidance specific to Tier 1 (e.g., threats related to organizational governance, core missions/business functions, management/operational policies, procedures, and structures, external mission/business relationships).
- Taxonomy of threat sources, annotated by the organization, if necessary. (**Table D-2**)
- Characterization of adversarial and non-adversarial threat sources.
  - Assessment scales for assessing adversary capability, intent, and targeting, annotated by the organization, if necessary. (**Table D-3, Table D-4, Table D-5**)
  - Assessment scale for assessing the range of effects, annotated by the organization, if necessary. (**Table D-6**)
- Threat sources identified in previous risk assessments, if appropriate.
	No	Yes	Yes
			if not provided by Tier 2

From Tier 2: (Mission/business process level) - Threat source information and guidance specific to Tier 2 (e.g., threats related to mission/business processes, EA segments, common infrastructure, support services, common controls, and external dependencies). - Mission/business process-specific characterization of adversarial and non-adversarial threat sources.	Yes *via RAR*	Yes *via peer sharing*	Yes
From Tier 3: (Information system level) - Threat source information and guidance specific to Tier 3 (e.g., threats related to information systems, information technologies, information system components, applications, networks, environments of operation). - Information system-specific characterization of adversarial and non-adversarial threat sources.	Yes *via RAR*	Yes *via RAR*	Yes *via peer sharing*

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 minaccia 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.
- Consideriamo solamente il danneggiamento degli asset dovuto a perdita o danneggiamento degli asset informativi con un impatto alto 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 del nist 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 entro quello desiderato

- Per condurre un'analisi del rischio efficace per l'azienda Alpha, è importante seguire un approccio strutturato. Ecco una possibile struttura per l'analisi del rischio:

- **Scopo**: L'obiettivo principale dell'analisi del rischio è identificare, valutare e mitigare i rischi associati agli attacchi informatici da parte del gruppo criminale organizzato.

- **Ambito**: L'analisi del rischio si concentrerà sull'infrastruttura IT dell'azienda, inclusi i sistemi basati su cloud, le applicazioni web e i dispositivi mobili. Inoltre, l'analisi si concentrerà sui dati sanitari sensibili gestiti dall'azienda.

- **Ipotesi**: Si presume che il gruppo criminale continuerà a cercare di esfiltrare i dati sanitari degli utenti. Inoltre, si presume che l'azienda continuerà a essere un obiettivo attraente per il gruppo criminale a causa della natura sensibile dei dati che gestisce.

- **Vincoli**: L'azienda può accettare solo un rischio basso per tutti gli eventi di rischio identificati. Inoltre, l'azienda non ha abilitato l'autenticazione multifattore (MFA) e non effettua regolarmente la valutazione delle vulnerabilità.

I RISK ASSESSMENT PER L'AZIENDA ALPHA, SEGUENDO GLI STEP 1 E 2 DEL NIST SP 800-30.

- **Step 1: Prepare for Assessment**
- Scopo: Identificare e proteggere i dati sanitari sensibili gestiti dall'azienda Alpha.
- Ambito: L'intera infrastruttura IT dell'azienda Alpha, che include sistemi basati su cloud, applicazioni web e dispositivi mobili.
- Ipotesi: L'azienda Alpha è un target di un gruppo criminale organizzato che sta cercando di esfiltrare dati sanitari sensibili.
- Vincoli: L'azienda non ha abilitato MFA e non effettua regolarmente Vulnerability Assessment.
- **Step 2: Conduct Assessment**
- Identificazione delle fonti di minaccia e degli eventi: Il gruppo criminale organizzato è la principale fonte di minaccia. L'evento di minaccia è l'esfiltrazione di dati sanitari sensibili.

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

- Identificazione delle vulnerabilità e delle condizioni predisponenti: L'azienda non ha abilitato MFA e non effettua regolarmente Vulnerability Assessment. Queste sono le principali vulnerabilità.

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

- Determinazione della probabilità di occorrenza: Data la continua sorveglianza del gruppo criminale e la mancanza di MFA e di Vulnerability Assessment, la probabilità di un attacco riuscito è alta.

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

- Determinazione dell'entità dell'impatto: Considerando solo il danneggiamento degli asset dovuto a perdita o danneggiamento degli asset informativi, l'impatto sarebbe alto.

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								

- Determinazione del rischio: Dato l'alto impatto e la probabilità di occorrenza, il rischio è alto.

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

- Per riportare il livello di rischio entro quello desiderato (basso), l'azienda dovrebbe considerare l'implementazione di MFA, l'esecuzione regolare di Vulnerability Assessment e l'adozione di altre misure di sicurezza per proteggere i dati sanitari sensibili. Inoltre, potrebbe essere utile lavorare con le autorità locali per affrontare la minaccia del gruppo criminale organizzato.

Tabella I-5

1	2	3	4	5	6	7	8	9	10	11	12	13
Threat Event	Threat Sources	Capability	Intent	Targeting	Relevance	Likelihood of Attack Initiation	Vulnerabilities and Predisposing Conditions	Severity and Pervasiveness	Likelihood Initiated Attack Succeds	Overall Likelihood	Level of Impact	Risk
E-5-1	D-7-1	High	Moderate	High	Confirmed	Very High	F-3-2	Moderate	Low	Moderate	High	Moderate
E-5-2	D-7-1	High	Moderate	High	Confirmed	Very High	F-3-2	Moderate	Low	Moderate	High	Moderate
E-5-3	D-7-1	High	Moderate	High	Confirmed	Very High	F-3-1	High	Moderate	High	High	High
E-5-4	D-7-1	High	Moderate	High	Confirmed	Very High	F-3-1	High	Moderate	High	High	High