Risk Assessment Alpha

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.

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 ulteriore 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 della 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 ricognizione sono attive, però lo scanning e sniffing portano a degli impatti bassi perchè 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

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.

Svolgimento

Lo Step 1, ovvero **Preparing for Risk Assessement**, si suddivide a sua volta in più step:

- Identify the purpose of the assessment
- Identify the scope of the assessment
- Identify the assumptions and constraints associated with the assessment
- Identify the sources of information to be used as inputs to the assessment
- Identify the risk model and analytic approaches (i.e., assessment and analysis approaches) to be employed during the assessment.

Identify the purpose of the assessment

Lo scopo di questo assessment è di valutare e comprendere i potenziali rischi per la sicurezza dei dati sanitari dell'azienda Alpha, derivanti da una minaccia esterna di un gruppo criminale organizzato. L'obiettivo è fornire una base per sviluppare e implementare misure di mitigazione del rischio.

Identify the scope of the assessment

Lo scope dell'assessment si concentrerà sulle potenziali minacce esterne dirette all'azienda, con particolare attenzione alle fasi iniziali della minaccia, visto che il gruppo criminale si trova nella fase di raccolta informazioni esterna. Si prenderanno in considerazione le attuali vulnerabilità attualmente presenti e le pratiche di sicurezza dell'azienda.

Identify the assumptions and constraints associated with the assessment

Supponiamo che l'azienda abbia un buon monitoraggio delle proprie reti e sistemi. Tuttavia è da prendere in considerazione che l'azienda non ha MFA attivo e non esegue Vulnerability Assessemnt periodici. Infine consideriamo che lo scopo dell'azienda è di mantenere un rischio basso per proteggere in particolare i dati sanitari sensibili dei propri pazienti.

Identify the sources of information to be used as inputs to the assessment

Fra le fonti di informazioni da usare troviamo: report di monitoraggio delle reti e dei sistemi, dati relativi alle pratiche di sicurezza attualmente attive, informazioni su minacce esterne e sulle tattiche specifiche del gruppo criminale coinvolto.

Identify the risk model and analytic to be employed during the assessment

In questo caso useremo il NIST SP 800-30 come modello di rischio, con focus sul Tier 3. Prenderemo in considerazione nello specifico le tabelle D-7 (Identify Threat Sources), E-5 (Determine Likelihood), F-3 (Determine Impact), F-6 (Determine Risk) H-4 (Determine Risk Response) e I-5 (Implement Risk Response). A queste ultime aggiungeremo valutazioni qualitative e quantitative delle probabilità e dell'impatto delle minacce identificate per determinare il livello complessivo di rischio e sviluppare risposte adeguate per ridurlo a un livello accettabile.

Lo Step 2, ovvero **Conducting the Risk Assessment**, si suddivide a sua volta in più step:

- Identify threat sources that are relevant to organizations
- Identify threat events that could be produced by those sources
- Identify vulnerabilities within organizations that could be exploited by threat sources through specific threat events and the predisposing conditions that could affect successful exploitation
- Determine the likelihood that the identified threat sources would initiate specific threat events and the likelihood that the threat events would be successful
- Determine the adverse impacts to organizational operations and assets, individuals, other organizations, and the Nation resulting from the exploitation of vulnerabilities by threat sources (through specific threat events)
- Determine information security risks as a combination of likelihood of threat exploitation of vulnerabilities and the impact of such exploitation, including any uncertainties associated with the risk determinations

Identify threat sources that are relevant to organizations

Usando il template della tabella D-7 identifichiamo le fonti di minaccia

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 (1)	Yes No	Table D-3 Organization -defined (2)	Table D-4 Organization -defined (3)	Table D-5 Organization -defined (4)

La fonte è di tipo Adversarial, nello specifico si tratta di un gruppo criminale organizzato

TABLE D-2: TAXONOMY OF THREAT SOURCES

Type of Threat Source	Description	Characteristics

ADVERSARIAL (1)
- Individual
  - Outsider
  - Insider
  - Trusted Insider
  - Privileged Insider
- Group
  - Ad hoc
  - Established
- Organization
  - Competitor
  - Supplier
  - Partner
  - Customer
- Nation-State
	Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).	Capability, Intent, Targeting

Dai dati si evince che l'avversario ha alte capacità di esperienza e risorse

TABLE D-3: ASSESSMENT SCALE – CHARACTERISTICS OF ADVERSARY CAPABILITY

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The adversary has a very sophisticated level of expertise, is well-resourced, and can generate opportunities to support multiple successful, continuous, and coordinated attacks.
2 High	80-95	8	The adversary has a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks.
			The adversary has moderate resources, expertise, and opportunities to support multiple successful

L'obiettivo è quello di rubare informazioni sensibili e creare persistenza quindi il livello d'intento è da considerarsi alto

TABLE D-4: ASSESSMENT SCALE – CHARACTERISTICS OF ADVERSARY INTENT

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The adversary seeks to undermine, severely impede, or destroy a core mission or business function, program, or enterprise by exploiting a presence in the organization's information systems or infrastructure. The adversary is concerned about disclosure of tradecraft only to the extent that it would impede its ability to complete stated goals.
3 High	80-95	8	The adversary seeks to undermine/impede critical aspects of a core mission or business function, program, or enterprise, or place itself in a position to do so in the future, by maintaining a presence in the organization's information systems or infrastructure. The adversary is very concerned about minimizing attack detection/disclosure of tradecraft, particularly while preparing for future attacks.
			The adversary seeks to obtain or modify specific critical or sensitive information or usurp/disrupt

Il bersaglio dell'avversario è chiaramente la compagnia Alpha quindi è di considerarsi di alto livello

TABLE D-5: ASSESSMENT SCALE – CHARACTERISTICS OF ADVERSARY TARGETING

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The adversary analyzes information obtained via reconnaissance and attacks to target persistently a specific organization, enterprise, program, mission or business function, focusing on specific high-value or mission-critical information, resources, supply flows, or functions; specific employees or positions; supporting infrastructure providers/suppliers; or partnering organizations.
4 High	80-95	8	The adversary analyzes information obtained via reconnaissance to target persistently a specific organization, enterprise, program, mission or business function, focusing on specific high-value or mission-critical information, resources, supply flows, or functions, specific employees supporting those functions, or key positions.
			The adversary analyzes publicly available information to target persistently specific high-value

Identify threat events that could be produced by those sources

Usando il template della tabella E-5 tentiamo di identificare i threat event che potrebbero scaturire

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 (1)	Table D-7, Table D-8 or Organization-defined	Table E-4 or Organization-defined (2)

Per la Threat Source possiamo fare riferimento alla tabella D-7 menzionata nelle precedenti pagine

Per il Threat Event usiamo la tabella E-3 e ipotizziamo dei possibili attacchi di Phishing per un primo foothold e per un eventuale persistenza nella rete

Craft or create attack tools.	
Craft phishing attacks. (1)	Adversary counterfeits communications from a legitimate/trustworthy source to acquire sensitive information such as usernames, passwords, or SSNs. Typical attacks occur via email, instant messaging, or comparable means; commonly directing users to websites that appear to be legitimate sites, while actually stealing the entered information.
Craft spear phishing attacks.	Adversary employs phishing attacks targeted at high value targets (e.g., senior leaders/executives).

Per la rilevanza usiamo la tabella E-4, in questo caso essendo note all'azienda le attività di ricognizione possiamo considerarla Confirmed

TABLE E-4: RELEVANCE OF THREAT EVENTS

Value	Description
Confirmed	The threat event or TTP has been seen by the organization. (2)
Expected	The threat event or TTP has been seen by the organization's peers or partners.

Identify vulnerabilities within organizations that could be exploited by threat sources through specific threat events and the predisposing conditions that could affect successful exploitation

Usando il template della tabella F-3 identifichiamo le vulnerabilità presenti nell'organizzazione e che potrebbero portare a una compromissione

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	1 Table F-2 or Organization-defined

Come fonti di vulnerabilità consideriamo:

- Mancanza di MFA (Multi Factor Authentication), il che facilità l'accesso non autorizzato
- Mancati Vulnerability Assessement periodici, che non permettono la scoperta e fix delle vulnerabilità già presenti
- Condivisione non supervisionata dei dati, anche sensibili, fra gli utenti, aumentando la superfice d'attaco
- Possibili malconfigurazioni del WAF (Web Application Firewall) che potrebbero creare nuovi vettori d'attacco

Per la severità delle vulnerabilità facciamo riferimento alla tabella F-2 e possiamo considerarle nell'insieme ad alto rischio

TABLE F-2: ASSESSMENT SCALE – VULNERABILITY SEVERITY

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The vulnerability is exposed and exploitable, and its exploitation could result in severe impacts. Relevant security control or other remediation is not implemented and not planned; or no security measure can be identified to remediate the vulnerability.
High 1	80-95	8	The vulnerability is of high concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is planned but not implemented; compensating controls are in place and at least minimally effective.

Utilizziamo la tabella F-6 per identificazione la condizioni predisposte

TABLE F-6: TEMPLATE – IDENTIFICATION OF PREDISPOSING CONDITIONS

Identifier	Predisposing Condition Source of Information	Pervasiveness of Condition
Organization-defined	1 Table F-4, Task 1-4 or Organization-defined	2 Table F-5 or Organization-defined

Per la fonte di informazioni usiamo la tabella F-4, che nel nostro caso si concentra principalmente sui dati sensibili

TABLE F-4: TAXONOMY OF PREDISPOSING CONDITIONS

Type of Predisposing Condition	Description
INFORMATION-RELATED - Classified National Security Information - Compartments - Controlled Unclassified Information - Personally Identifiable Information - Special Access Programs - Agreement-Determined - NOFORN - Proprietary	Needs to handle information (as it is created, transmitted, stored, processed, and/or displayed) in a specific manner, due to its sensitivity (or lack of sensitivity), legal or regulatory requirements, and/or contractual or other organizational agreements.
TECHNICAL	Needs to use technologies in specific ways

1

Per la pervasività utilizziamo la tabella F-5 che nel nostro caso possiamo considerare come alta

TABLE F-5: ASSESSMENT SCALE – PERVASIVENESS OF PREDISPOSING CONDITIONS

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Applies to **all** organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).
2 High	80-95	8	Applies to **most** organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).

Determine the likelihood that the identified threat sources would initiate specific threat events and the likelihood that the threat events would be successful

Per determinare la probabilità di possibili threat event e il loro successo usiamo le colonne 7, 10 e 11 della tabella I-5 poichè si tratta di un rischio di tipo Adversarial

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								
						1			2	3		

1. La probabilità di un attacco è da considerarsi alta vista la preparazione che sta effettuato il gruppo criminale
2. La probabilità di successo di un attacco iniziale può considerarsi Moderata considerando che l'organizzazione è già a conoscenza della minaccia e potrebbe prepararsi
3. La probabilità di successo generale dell'attacco è da considerarsi Alta visto il numero di vulnerabilità presenti visionate nelle pagine precedenti

Determine the adverse impacts to organizational operations and assets, individuals, other organizations, and the Nation resulting from the exploitation of vulnerabilities by threat sources (through specific threat events)

Per determinare l'impatto sugli asset usiamo il template della tabella H-4

TABLE H-4: TEMPLATE – IDENTIFICATION OF ADVERSE IMPACTS

Type of Impact	Impact Affected Asset	Maximum Impact
Table H-2 or Organization-defined (1)	Table H-2 or Organization-defined	(2) Table H-3 or Organization-defined

In questo caso visto che il bersaglio sono informazioni sensibili possiamo considerare come Asset principale queste ultime

TABLE H-2: EXAMPLES OF ADVERSE IMPACTS

Type of Impact	Impact

HARM TO OPERATIONS	- Inability to perform current missions/business functions.
	  - In a sufficiently timely manner.
	  - With sufficient confidence and/or correctness.
	  - Within planned resource constraints.
	- Inability, or limited ability, to perform missions/business functions in the future.
	  - Inability to restore missions/business functions.
	  - In a sufficiently timely manner.
	  - With sufficient confidence and/or correctness.
	  - Within planned resource constraints.
	- Harms (e.g., financial costs, sanctions) due to noncompliance.
	  - With applicable laws or regulations.
	  - With contractual requirements or other requirements in other binding agreements (e.g., liability).
	- Direct financial costs.
	- Relational harms.
	  - Damage to trust relationships.
	  - Damage to image or reputation (and hence future or potential trust relationships).

HARM TO ASSETS (1)	- Damage to or loss of physical facilities. - Damage to or loss of information systems or networks. - Damage to or loss of information technology or equipment. - Damage to or loss of component parts or supplies. - Damage to or of loss of information assets. - Loss of intellectual property.
HARM TO INDIVIDUALS	- Injury or loss of life.

L'impatto degli eventi è di considerarsi serio e quindi Moderate secondo la tabella H-3 perchè rappresenta un danno significativo agli Asset aziendali

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.
2 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.

Determine information security risks as a combination of likelihood of threat exploitation of vulnerabilities and the impact of such exploitation, including any uncertainties associated with the risk determinations

Per riassumere il tutto I rischi per la sicurezza delle informazioni sono da considerarsi elevati, data l'alta probabilità di sfruttamento delle vulnerabilità, e dato l'impatto significativo che tale sfruttamento potrebbe avere sull'azienda e i suoi clienti e organizzazioni collegate

Azioni per la mitigazione del rischio

- Implementazione del MFA per diminuire notevolmente gli accessi non autorizzati
- Esecuzione di Vulnerability Assessment periodici per trovare e ridurre il più possibile le vulnerabilità
- Implementazione di controlli di sicurezza avanzati visto che si ci trova di fronte a un gruppo ben organizzato
- Miglioramento della formazione sulla sicurezza per educare il personale contro gli attacchi più pericolosi come il Phishing
- Limitazione dell'accesso ai dati sensibili per diminuire la superfice d'attacco
- Revisione delle policy di sicurezza per adattarle alla minaccia incombente