BCC – Risk Management

Progetto settimanale
S02 – L05

Davide
Andreozzi

Agenda


Introduzione
Prepare For Assessment
Conduct Assessment
Livelli di Rischio
Considerazioni sul rischio

Traccia

EPICODE

Risk Management
Progetto

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.

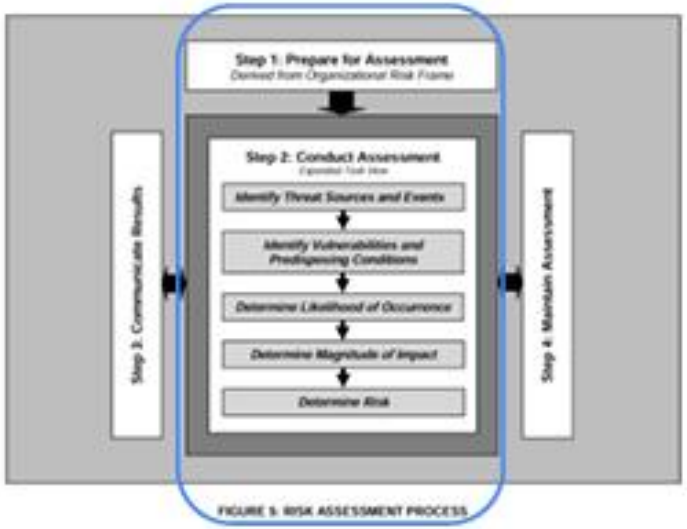

FIGURE 5: RISK ASSESSMENT PROCESS

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*

Traccia

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.

Traccia

EPICODE

Risk Management
Progetto

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.

Prepare for Assessment

- Scopo del Risk Assessment:
  - Lo scopo di questo Risk Assessment è la protezione degli asset principali che contengono dati sanitari e informazioni sensibili dei clienti.
- Ambito del Risk Assessment:
  - Infrastruttura IT critica:
    - Server e database interno
    - Applicativo aziendale che consente la condivisione dei dati sensibili

Conduct Assessment – Identify threat sources

Basandoci sulla tabella D-7 e sulle informazioni che abbiamo possiamo identificare come fonte di minaccia avversaria il gruppo di criminali che tiene sotto controllo gli asset e l'organizzazione.

Facendo un analisi con il supporto delle tab D-3, D-4 e D-5 possiamo identificare tramite la seguente tabella il livello di capacità, intento e obbiettivo degli hacker.

Capacità	Intento	Obbiettivo
Moderata	Moderato	Alto

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

Conduct Assessment – Identify threat events

Andiamo in questo caso a trovare i possibili Threat Events:

- Attacco di ingegneria sociale tramite phishing
- Attacco DDoS per bypassare i dispositivi di sicurezza
- Invio Malware per l'esfiltrazione dei dati sensibili
- Attacco Brute-Force agli account del personale

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

Conduct Assessment – Identify vulnerabilities and predisposing conditions

Vulnerabilità

- Possibile CVE sull'applicativo aziendale (Alta)
- Database non crittografato (Medio-Alta)
- 2MFA non implementata (Alta)
- Configurazioni Firewall non ottimali (Media)

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

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

Conduct Assessment – Determine Impact

Il verificarsi dell'evento porterà principalmente tre tipi di impatto

- Danno alle operazioni
  - Potrebbe ridurre o bloccare l'operatività aziendale
  - Applicazione di sanzioni da organi di controllo in materia di data privacy e gestione delle informazioni
  - Perdita di reputazione e credibilità aziendale
  - Perdita economica diretta e indiretta
- Danno agli asset
  - Perdita di dati
- Danno alle altre organizzazioni

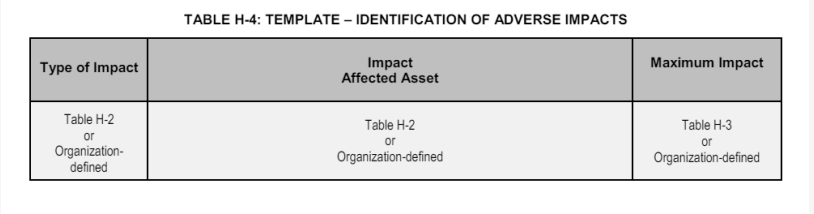

TABLE H-4: TEMPLATE – IDENTIFICATION OF ADVERSE IMPACTS

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

Threat Event	Threat Sources	T.S.C Capacità	T.S.C. Intento	T.S.C. Obbiettivo	Rilevanza	Probabilità	Vulnerabilità e condizioni Predisponenti	Severità e Perseveranza	Probabilità di successo	Probabilità complessiva	Livello di Impatto	Rischio
Phishing	Hacker	Moderato	Moderato	Alto	Predicted	Moderata	Dipendenti	Media	Bassa	Moderata	Moderato	Moderato
DDoS	Hacker	Moderato	Moderato	Alto	Anticipated	Molto Bassa	Firewall non configurato	Media	Bassa	Molto bassa	Basso	Molto basso
Malware	Hacker	Moderato	Moderato	Alto	Predicted	Bassa	CVE + Database non crittografato	Alta	Alta	Alta	Alto	Alto
Brute-Force	Hacker	Moderato	Moderato	Alto	Anticipated	Alta	2MFA Assente	Alta	Moderata	Moderata	Alto	Moderato

Date i diversi Threat Events possiamo definire i seguenti rischi:

- Rischio Alto:
    - Il Threat Event associato a questo livello di rischio è il **Malware**,
    - Il livello di rischio alto non è ritenuto accettabile da parte dell'organizzazione
  - Azioni da attuare: Patching OS, Database e Applicativo aziendale, Crittografia di tutte le informazioni sul database e nella condivisione sull'applicativo.
- Rischio Moderato
    - I Threat Events associati a questo livello di rischio sono il **Phishing** e il **Brute-Force**
    - Il livello di rischio moderato non è ritenuto accettabile da parte dell'organizzazione
  - Azioni da attuare: Miglioramento della formazione del personale, implementazione di regole di firewall più idonee e implementazione di sistemi IDPS, implementazione di politica seria di autenticazione aziendale e introduzione del 2MFA tramite token HW.
- Rischio Molto Basso
    - Il Threat Event associato a questo livello di rischio è il DDoS
    - Il livello di rischio «molto-basso» è ritenuto accettabile da parte dell'organizzazione
  - Azioni da attuare: Monitoraggio continuo della minaccia per verificare se il livello di rischio cambia, nessun'azione di mitigazione da effettuare.

Grazie