Progetto BCC Iccrea – S2/L5

Traccia:

Simulare un processo di Risk Assessment, solo Step 1 e Step 2 (tralasciando Step 3 e Step 4), seguendo NIST SP 800-30, considerate solo le sorgenti del Tier 3.

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

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.

Il processo di risk assessment è composto da quattro fasi: preparazione; conduzione; comunicazione dei risultati dell'assessment e mantenimento. Come già definito noi ci concentreremo sui primi due step:

1. Prepare for Assessment, la prima fase è formata da 5 attività:

1.Identificare lo scopo del risk assessment → valutare i rischi per l'azienda Alpha derivanti dalle minacce esterne, in particolare quelle provenienti da un gruppo criminale ben organizzato, il cui scopo è quello di compromettere la sicurezza dei dati sanitari andandoli ad esfiltrare e compromettendo i servizi online dell'azienda.

2.Identificare l'ambito del risk assessment → Copre tutti i sistemi informativi e le infrastrutture IT utilizzate per la gestione dei dati sanitari e l'erogazione dei servizi online.

3.Identificare le ipotesi e i vincoli in base ai quali viene condotta il risk assessment →

Ipotesi: Il gruppo criminale ha le risorse e le capacità per condurre attacchi sofisticati e coordinati contro l'azienda Alpha, la quale non ha implementato MFA e non effettua regolarmente Vulnerability Assessment; mentre scanning e sniffing hanno impatti bassi a causa della presenza di un firewall e di un WAF su cloud.

Vincoli: L'azienda Alpha può accettare solo un rischio basso per tutti gli eventi di rischio identificati, considerando il valore critico dei dati sanitari dei pazienti.

4.Identificare sorgenti di informazioni per threat, vulnerabilità e impatti da utilizzare nella valutazione del rischio (tabelle D-1, E-1, F-1, H-1, I-1).

Tabella D1 (threat source identification): Ci fornisce informazioni sulle fonti di minaccia, utilizzate per comprendere le minacce esterne che potrebbero essere dirette verso l'infrastruttura IT e i dati sanitari dell'azienda Alpha.

Fonti di minaccia credibili: Rapporti di intelligence sulle minacce provenienti da gruppi criminali organizzati che mirano ai fornitori di servizi sanitari online. Fonti: NVD, CVE, CVSS, questionati e interviste al personale dipendente, penetration testing.

Fonti di minaccia classificati: Rapporti governativi o di agenzie di intelligence che indicano un aumento delle attività di hacking nel settore sanitario.

Tabella E1 (threat event identification): Fornisce informazioni sugli eventi di minaccia, che potrebbero avere un impatto sui sistemi informativi dell'azienda, come attacchi informatici mirati alla violazione dei dati sanitari.

Attacchi informatici mirati: Rapporti di incidenti precedenti che mostrano tentativi di accesso non autorizzato ai sistemi IT dell'azienda Alpha. Ad esempio, rapporti di incidenti

precedenti potrebbero fornire informazioni sulle minacce di sicurezza informatica che potrebbero bypassare il firewall e il WAF su cloud.

Violazioni dei dati sanitari: Incidenti di perdita o furto di dati sanitari di pazienti registrati nei sistemi dell'azienda.

Tabella F1 (vulnerabilities and predisposing conditions): Fornisce informazioni sulle vulnerabilità e sui rischi identificati per l'uso a livello organizzativo. Queste informazioni sono cruciali per identificare le potenziali debolezze nei sistemi IT dell'azienda Alpha che potrebbero essere sfruttate dagli attaccanti.

Vulnerabilità dei software non aggiornati: Segnalazioni di sicurezza che indicano che alcuni software utilizzati dall'azienda Alpha non sono aggiornati con le patch di sicurezza più recenti.

Scarsa protezione dei dati: Risultati di una valutazione della sicurezza che evidenziano configurazioni errate o mancanti di firewall o controlli di accesso ai dati.

Tabella H1 (determination of impact): Fornisce informazioni sull'impatto, sono dunque importanti per comprendere le possibili conseguenze degli eventi di minaccia sui sistemi informativi e sull'operatività dell'azienda Alpha.

Perdita di dati sanitari: Stimare l'impatto finanziario e reputazionale di una violazione dei dati sanitari che coinvolge migliaia di pazienti dell'azienda Alpha.

Interruzione dei servizi: Valutare l'impatto operativo di un attacco informatico che compromette la disponibilità dei servizi sanitari online offerti dall'azienda.

Tabella I1 (risk): Fornisce informazioni sul rischio e sull'incertezza e aiutano a valutare il livello complessivo di rischio associato alle minacce e alle vulnerabilità identificate.

Rischio di valutazione dei dati: Combinare la probabilità di un attacco informatico mirato con l'impatto finanziario e reputazionale di una violazione dei dati per valutare il rischio complessivo per l'azienda Alpha.

Rischio di perdita di disponibilità del servizio: Valutare la probabilità di un attacco DDoS mirato e il relativo impatto sulla disponibilità dei servizi sanitari online.

5.Definire o perfezionare il modello di rischio, l'approccio di assessment e l'approccio di analisi nella valutazione del rischio →

Modello di rischio → Considerando l'azienda Alpha, il modello di rischio dovrebbe concentrarsi sulla valutazione delle minacce specifiche legate alla gestione dei dati sanitari sensibili e all'erogazione dei servizi sanitari online. Potrebbe includere categorie di minacce come attacchi informatici, violazioni dei dati, interruzioni dei servizi, e categorie di impatto

come finanziario, reputazionale e sulla salute dei pazienti. Considerando l'efficacia del firewall e del WAF su cloud nel mitigare gli impatti degli attacchi di scanning e sniffing, il modello di rischio dovrebbe tener conto di queste contromisure e concentrarsi sulle minacce che potrebbero superarle.

Approccio di assessment → Approccio basato sulle migliori pratiche del settore sanitario e delle tecnologie dell'informazione, questo potrebbe includere l'uso di metodologie standard come il Framework NIST per la Cybersecurity e il trattamento dei dati sensibili in conformità con le normative come il GDPR nel contesto europeo o l'HIPAA negli Stati Uniti.

Approccio di analisi → L'analisi dovrebbe concentrarsi sull'identificazione delle minacce più rilevanti e delle vulnerabilità più critiche per i dati sanitari, nonché sull'identificazione delle contromisure più efficaci per mitigare tali rischi, attraverso l'uso coinvolgere di analisi quantitative e qualitative per valutare la probabilità e l'impatto delle minacce, concentrandosi sulle vulnerabilità critiche che potrebbero essere sfruttate nonostante le contromisure.

Arriviamo alla seconda fase del processo di risk assessment, ovvero:

2.Conduzione dell'assessment: con l'aiuto delle tabelle NIST 800-30

Tabella D7: implementata con l'ausilio di D2, D3, D4, D5

TABLE D-2: TAXONOMY OF THREAT SOURCES

Type of Threat Source	Description	Characteristics

ADVERSARIAL
- 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

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

Identifier	Threat Source	In scope	Capability	Intent	Targeting
D7-A	Adversarial (group) Gruppo criminale organizzato	yes	High	Very high	high

Tabella E5: con l'ausilio di E2, E3, D5, D8, E4

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

Identifier	Threat event	Threat source	Relevance
E5-A	Effettuare ricognizione e scansione della rete perimetrale	Adversarial (group)	Confirmed
E5-B	Effettuare sniffing della rete esposta	Adversarial (group)	Confirmed
E5-C	Raccogliere informazioni tramite scoperta open source	Adversarial (group)	Expected
E5-D	Effettuare ricognizione e sorveglianza delle organizzazioni target	Adversarial (group)	Anticipated
E5-E	Creare attacchi di phishing	Adversarial (group)	Expected
E5-F	Ottenere informazioni sensibili tramite esfiltrazione	Adversarial (group)	Predicted

Tabella F3:

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

Identifier	Vulnerability	Vulnerability severity
F3-A	Assenza di MFA	High
F3-B	Mancanza di monitoraggio adeguato	High

Tabella F6:

Identifier	Predisposing condition – Source of information	Pervasiveness of condition
F6-A	Information related: - Informazioni Classificate per la Sicurezza Nazionale - Informazioni di Identificazione Personale	-Molto alta (10) -Moderata (5)
F6-B	Technical: -Conformità agli Standard Tecnici	-Alta (8)
F6-C	Operational/Environmental -Mobility/semi mobility -La popolazione con accesso fisico e/o logico ai componenti del sistema informativo	-Moderata (5) -Molto alta (10)

Information related: Considerando la gestione dei dati sanitari, la condizione predisponente più appropriata potrebbe essere "Informazioni Classificate per la Sicurezza Nazionale" con una pervasività molto alta; anche se potrebbe sembrare che i dati sanitari non siano direttamente correlati alla sicurezza nazionale, è importante considerare che i dati sanitari sono estremamente sensibili e devono essere trattati con la massima riservatezza e protezione.

Technical: La conformità agli standard tecnici è valutata con un alto livello di pervasività. Ciò indica che Alpha deve rispettare rigorosi standard tecnici, probabilmente per garantire la sicurezza e l'integrità dei dati.

Operational / Environmental: La mobilità, in particolare il tipo semi-mobile, ha un livello di pervasività moderato. Questo potrebbe indicare che parte del personale di Alpha opera in ambienti mobili o remoti, influenzando le modalità di accesso e gestione delle informazioni. Mentre la popolazione con accesso fisico e/o logico ai componenti del sistema informativo ha un alto livello di pervasività, ciò suggerisce che ci sono molte persone all'interno dell'organizzazione che hanno accesso ai sistemi informativi di Alpha, il che potrebbe aumentare il rischio di accessi non autorizzati o di perdita di dati sensibili.

Tabella H4:

Type of Impact	Impact – Affected Asset	Maximum Impact
Harm to operations	Interruzione dei servizi sanitari a causa dell'indisponibilità dei dati.	Elevato (8)
Harm to asset	Accesso non autorizzato ai dati sanitari, compromettendo la loro integrità.	Molto Alto (10)
Harm to individuals	Esposizione dei dati sanitari sensibili, aumentando il rischio di furto di identità medica.	Molto Alto (10)
Harm to organization	Possibili sanzioni e multe a causa della violazione della normativa sulla privacy dei dati.	Moderato (5)
Harm to the nation	Perdita di fiducia nel sistema sanitario nazionale a causa di violazioni della privacy.	Moderato (5)

Tabella I5:

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								

Threat event	Threat source	Capability	Intent	Targeting Relevance	Likelihood of attack Initiation
E5-A	D7-A	High	High	Very high	Confirmed
E5-B	D7-A	High	High	Very high	Confirmed
E5-C	D7-A	High	High	Very high	Expected
E5-D	D7-A	High	High	Very high	Anticipated
E5-E	D7-A	Moderate	Moderate	High	Expected
E5-F	D7-A	Moderate	Moderate	High	Predicted

Vulnerabilities and predisposing conditions	Severity and pervasiveness	Likelihood initiated attack succeds	Overall likelihood	Level of impact	Risk
F3-A	High	Medium	Moderate	Very high	Very high
F3-A	High	Medium	Moderate	Very high	Very high
F3-A	High	Medium	Moderate	High	High
F3-B	Moderate	Low	High	High	High
F3-B	Moderate	Low	High	High	High
F3-B	Moderate	Low	High	High	High

Soluzioni per mitigazione del rischio (da alto a basso) per per tutti gli eventi di rischio identificati, dovuto al valore del loro asset principale «dati sanitari».

Implementazione di contro misure: Attuare misure di sicurezza specifiche per mitigare o ridurre le vulnerabilità e le condizioni predisponenti identificate. Questo potrebbe includere l'aggiornamento dei firewall, l'implementazione dell'autenticazione a due fattori, l'adozione di filtri anti-phishing, la crittografia dei dati sensibili.

Formazione personale: Fornire formazione e sensibilizzazione al personale sull'importanza della sicurezza informatica e sulle migliori pratiche per proteggere i dati sensibili, come riconoscere e evitare gli attacchi di phishing + maggiore comunicazione e coinvolgimento attivo di tutte le parti interessate, inclusi i dipendenti, i partner commerciali e gli esperti esterni, nella gestione della sicurezza informatica e nella mitigazione dei rischi.

Controlli e monitoraggio continui: Implementare un sistema di monitoraggio costante delle attività di rete e dei comportamenti anomali per rilevare e rispondere tempestivamente alle minacce. Inoltre, è essenziale rivedere periodicamente le misure di sicurezza implementate per garantire che siano efficaci e aggiornate.

Risposta degli incidenti: Sviluppare e testare un piano di risposta agli incidenti per gestire prontamente eventuali violazioni della sicurezza e mitigare i danni in caso di compromissione dei dati.

Valutazione del rischio continua: Condurre valutazioni periodiche del rischio per identificare eventuali nuove minacce o vulnerabilità e adattare le contromisure di conseguenza.