RISK ASSESTMENT REPORT

All’attenzione di: Bruce Wayne, C.O. di Apha Healthcare
Preparato da: Oliviero Camarota
8 maggio 2024

RIEPILOGO ESECUTIVO

Finalità

L’obbiettivo di oggi é quello di simulare un processo di Risk Assestment, seguendo le step 1 e 2 del NIST SP 800-30 rev.1, per il Tier 3.

Obiettivi

Fornire una valutazione completa dei rischi di sicurezza che impattano le operazioni di Alpha Healthcare, concentrandosi particolarmente sui dati sanitari sensibili gestiti dall'azienda.

Indice

1 - Contesto Aziendale

Lo scenario a cui verra applicato il processo di valutazione del rischio è il seguente:

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 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 Assestment.
- 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 WAF su cloud, invece gli effetti potrebbero essere moderai nella ricerca open source o nella sorveglianza di alcuni target particolari.
- Considerando solamente il danneggiamento degli asset dovuto a perdita o danneggiamento degli asset informativi, con un impatto alto.

Ipotizzare che l'organizzazione possa accettare solamente un rischio basso per tutti gli eventi di rischio identificati, dovuto al valore del loro asset principali << dati sanitari>>. Fate delle valutazioni e delle ipotesi sui prossimi passaggi da eseguire per riportare il livello di rischio ottenuto entro quello desiderato.

2 - Preparazione per la Valutazione del Rischio di Alpha Healthcare

La prima fase del processo di valutazione del rischio consiste nella preparazione dell'analisi. L'obiettivo di questa fase è stabilire un contesto per la valutazione del rischio, basandosi sui risultati della fase di definizione del rischio del processo di gestione del rischio. Questa preparazione si basa sulle politiche organizzative, le metodologie di valutazione specifiche, e le procedure che influenzano la selezione dei fattori di rischio, l'ambito delle valutazioni, il rigore delle analisi, e il grado di formalità necessari per ottenere determinazioni del rischio coerenti e ripetibili. Le informazioni ottenute dalla strategia di gestione del rischio aiutano a organizzare la fase di preparazione, che include i seguenti compiti essenziali:

- Identificare lo scopo della valutazione:
Valutare specificamente i rischi associati alla sicurezza dei dati sanitari sensibili gestiti da Alpha Healthcare, focalizzandosi sulla protezione di questi dati dalle minacce esterne, in particolare dai gruppi criminali organizzati.

- Identificare l'ambito della valutazione:
L'analisi sarà concentrata esclusivamente sulla sicurezza dei dati sanitari sensibili, includendo tutte le piattaforme e sistemi che trattano tali dati, sia fisici che digitali.

- Identificare le ipotesi e i vincoli associati alla valutazione:
Ipotesi: I gruppi criminali organizzati hanno l'obiettivo di esfiltrare dati sanitari senza essere rilevati.
Vincoli: L'analisi è limitata dalle capacità correnti di sicurezza IT e dalla mancanza di un sistema MFA (Multi-Factor Authentication) già implementato.

- Identificare le fonti di informazione da utilizzare come input per la valutazione:
Fonti includeranno i dati dai sistemi di monitoraggio della sicurezza, i rapporti di valutazione del rischio precedenti, le politiche di sicurezza vigenti, e i feedback dalle revisioni di sicurezza interne.

- Identificare il modello di rischio e gli approcci analitici da impiegare durante la valutazione:
Modello di rischio: Sarà focalizzato sulla probabilità di attacchi riusciti e sull'impatto di tali attacchi sulla riservatezza e l'integrità dei dati sanitari.

2.1 - Identificazione dello scopo

Basandosi sulle direttive dettagliate dal NIST SP 800-30 per la valutazione del rischio, possiamo specificare lo scopo della valutazione del rischio per Alpha Healthcare in termini di informazioni da produrre e decisioni da supportare. La valutazione è progettata per garantire che le informazioni prodotte siano appropriate e supportino decisioni ben informate a vari livelli organizzativi.

Di seguito, si delineano gli scopi specifici di questa valutazione del rischio, tenendo conto sia di valutazioni iniziali che di riesami:

- Stabilire una Valutazione di Base del Rischio:
Produrre una valutazione di base dei rischi associati alla gestione dei dati sanitari sensibili, includendo la mappatura delle minacce, delle vulnerabilità e degli impatti potenziali sulle operazioni organizzative, sugli individui, e sulla sicurezza nazionale.

- Identificazione delle Minacce e delle Vulnerabilità:
Identificare minacce e vulnerabilità specifiche che potrebbero influenzare i sistemi di informazione che supportano i processi di missione/affari di Alpha Healthcare.

- Aggiornamento della Valutazione del Rischio:
Aggiornare la valutazione del rischio in risposta a cambiamenti nei sistemi di informazione o negli ambienti operativi, come modifiche hardware, software, controlli specifici del sistema, processi di missione/affari, infrastrutture comuni e servizi di supporto, nonché nuove minacce e vulnerabilità.

2.2 Identificazione dell’ambito

Per Alpha Healthcare, identificare l'ambito della valutazione del rischio è cruciale per assicurare che le decisioni basate sul rischio siano informate e pertinenti.

L'ambito della valutazione del rischio coprirà tutti gli aspetti dell'organizzazione che riguardano la gestione e la protezione dei dati sanitari sensibili. Questo include:

- **Sistemi Informativi**: Tutti i sistemi informatici utilizzati per la raccolta, lo stoccaggio, il processamento e la trasmissione dei dati sanitari.
- **Processi di Missione/Aziendali**: Processi specifici legati alla fornitura di servizi sanitari online e al supporto cliente.
- **Controlli di Sicurezza**: Selezione, personalizzazione e integrazione dei controlli di sicurezza che proteggono i sistemi informatici e i dati.

Ambito Temporale di Efficacia

- **Decisioni di Politica a Livello Tier 1**: Considerando la natura critica dei dati sanitari e le implicazioni di conformità, i risultati della valutazione del rischio dovranno rimanere rilevanti per un periodo prolungato, data la lentezza del processo di governance e di cambiamento delle politiche in molte organizzazioni.
- **Decisioni Operative a Livello Tier 3**: Le valutazioni che informano l'uso di controlli di sicurezza compensativi per i sistemi informativi potrebbero essere rilevanti solo fino al rilascio successivo del prodotto tecnologico che fornisce la capacità di sicurezza richiesta.

Considerazioni Architettoniche e Tecnologiche

- **A Livello di Tier 3**: L'ambito di valutazione del rischio sarà focalizzato sui sistemi informativi specifici di Alpha Healthcare nel loro ambiente operativo, prendendo in considerazione le vulnerabilità dei controlli ereditati.
- **A Livello di Tier 2**: Per una valutazione mirata, l'ambito può essere definito in termini di architettura del segmento missione/aziendale, includendo tutti i sistemi, i servizi e le infrastrutture che supportano una specifica funzione missione come la gestione dei dati sanitari.

2.3 - Identificazione ipotesi e vincoli

Per la valutazione del rischio di Alpha Healthcare, considerando le specificità del contesto aziendale, è essenziale identificare chiaramente le ipotesi e i vincoli che influenzano il processo di valutazione. Questo passo è cruciale per garantire che la valutazione sia realistica e allineata con le capacità e le esigenze dell'organizzazione. Di seguito sono delineate le ipotesi e i vincoli rilevanti per la valutazione del rischio in Alpha Healthcare:

Ipotesi

1. **Fonti di Minaccia**:
   - Si presume che il principale pericolo provenga da gruppi criminali organizzati con capacità avanzate e risorse per condurre attacchi sofisticati, mirati all'esfiltrazione di dati sanitari.
2. **Eventi di Minaccia**:
   - Si considerano eventi di minaccia che hanno già manifestato una forma di attacco verso organizzazioni simili nel settore sanitario, inclusi phishing, attacchi ransomware, e violazioni dei dati.
3. **Vulnerabilità e Condizioni Predisponenti**:
   - Si ipotizza che le principali vulnerabilità siano legate a sistemi IT non aggiornati, mancanza di MFA, e insufficiente formazione del personale su pratiche di sicurezza informatica.
4. **Impatti**:
   - Gli impatti sono valutati soprattutto in termini di perdita di integrità e riservatezza dei dati sanitari, con potenziali conseguenze legali e danni alla reputazione di Alpha Healthcare.
5. **Approcci di Valutazione e Analisi**:
   - Si utilizzeranno approcci qualitativi e semi-quantitativi per la valutazione del rischio, data la difficoltà di quantificare esattamente alcuni tipi di impatti e la probabilità di eventi di minaccia.

Vincoli

1. **Risorse Disponibili**:
   - Le risorse finanziarie e umane disponibili per la valutazione del rischio sono limitate, influenzando la profondità e la frequenza delle valutazioni di sicurezza.
2. **Competenze e Expertise**:
   - Si riconosce una carenza di competenze specializzate in cybersicurezza all'interno dell'organizzazione, necessitando quindi il supporto esterno o la formazione interna per colmare questo gap.
3. **Considerazioni Operative**:
   - Le attività di valutazione del rischio devono minimizzare l'interruzione delle operazioni aziendali quotidiane, particolarmente critiche in un contesto di servizi sanitari online.
4. **Tolleranza al Rischio**:
   - Data la sensibilità dei dati gestiti, Alpha Healthcare ha una bassa tolleranza al rischio, particolarmente per i rischi che potrebbero compromettere i dati dei pazienti.
5. **Incertezza**:
   - Esiste una significativa incertezza riguardo alla probabilità di nuovi tipi di attacchi cibernetici e alla efficacia delle misure di sicurezza adottate di recente, dovuta alla rapida evoluzione delle minacce e delle tecnologie.

2.4 - Identificazione fonti di informazione

Per Alpha Healthcare, la valutazione del rischio richiederà l'utilizzo di diverse fonti di informazioni per descrivere accuratamente il contesto, identificare minacce e vulnerabilità, e valutare gli impatti. Ecco una panoramica delle fonti di informazioni che possono essere utilizzate in base ai livelli descritti:

Fonti di Informazioni Descrittive

- **Governance della Gestione del Rischio e della Sicurezza Informatica**: Documenti interni che dettagliano le strutture di gestione del rischio e di sicurezza informatica, come le politiche di sicurezza e i framework operativi.
- **Processi di Missione/Aziendali**: Documentazione sui processi aziendali, flussi di informazioni e responsabilità funzionali, particolarmente quelli che impattano o sono legati alla gestione dei dati sanitari.
- **Architettura dell'Impresa e Sicurezza**: Piani di architettura aziendale e documentazione sulla sicurezza che descrivono i sistemi, le infrastrutture comuni e i servizi condivisi che rientrano nell'ambito della valutazione del rischio.

Fonti di Informazioni sulle Minacce

- **Interni**: Report di valutazione del rischio, report di incidenti, log di sicurezza e risultati di monitoraggio che possono fornire insight sulle minacce attuali e potenziali
- **Esterni**: Organizzazioni come US-CERT, DCISE, ISACs, e altre entità settoriali o di ricerca come il Software Engineering Institute-CERT che offrono avvisi di sicurezza, analisi delle minacce e raccomandazioni di mitigazione.

Fonti di Informazioni sulle Vulnerabilità

- **Interni**: Report di valutazione delle vulnerabilità, audit interni e controlli di sicurezza che dettagliano le vulnerabilità attuali nei sistemi informatici.
- **Esterni**: Fonti esterne simili a quelle delle minacce, che possono fornire dati su nuove vulnerabilità e modalità di attacco emergenti.

Fonti di Informazioni sugli Impatti

- **Interni**: Analisi di impatto sul business, inventari dei componenti dei sistemi di informazione, e valutazioni delle categorie di sicurezza che determinano gli impatti potenziali degli eventi di sicurezza.
- **Esterni**: Studi di settore, benchmarking e ricerche pubblicate che possono offrire una panoramica degli impatti di incidenti simili in altre organizzazioni o settori.

L'utilizzo di queste fonti di informazioni permetterà ad Alpha Healthcare di avere una valutazione del rischio completa e informata, che aiuterà l'organizzazione a comprendere meglio i rischi per la sicurezza e a implementare misure di mitigazione efficaci. Le informazioni raccolte dovrebbero essere aggiornate regolarmente per mantenere la valutazione del rischio rilevante e accurata, riflettendo il dinamico panorama delle minacce e delle vulnerabilità nel settore sanitario.

2.5 - Identificazione del modello di rischio e dell’approccio analitico

Per la valutazione del rischio presso Alpha Healthcare, ci focalizzeremo esclusivamente sull'uso di un'analisi qualitativa, il modello di rischio e l'approccio analitico saranno progettati per facilitare decisioni basate su una comprensione profonda delle minacce, delle vulnerabilità e degli impatti senza l'uso di dati numerici dettagliati.

Modello di Rischio

Fattori di Rischio:

- **Minacce**: Identificazione delle minacce che possono compromettere i dati sanitari sensibili e le operazioni di Alpha Healthcare. Le minacce verranno classificate in base alla loro origine (es., interna, esterna), tipo (es., intenzionale, accidentale) e frequenza di occorrenza passata.
- **Vulnerabilità**: Esame delle debolezze attuali che possono essere sfruttate dalle minacce. Queste vulnerabilità saranno catalogate in termini di gravità e facilità di sfruttamento.
- **Impatti**: Valutazione degli effetti negativi che potrebbero risultare dall'esploitazione delle vulnerabilità da parte delle minacce, considerando tanto la perdita di dati e di funzionalità quanto gli impatti sulla reputazione e sulla conformità legale.
- **Probabilità**: Determinazione della frequenza con cui le minacce identificate potrebbero effettivamente sfruttare le vulnerabilità disponibili.

Approccio Analitico Qualitativo

- Valutazione delle Minacce: Utilizzo di informazioni raccolte da fonti interne ed esterne per identificare e descrivere le minacce potenziali. Si valuterà la plausibilità delle minacce basandosi su esperienze passate e intelligenza di settore.

- **Valutazione delle Vulnerabilità**: Analisi delle debolezze nei sistemi IT che possono essere sfruttate da attori malintenzionati. Questo processo includerà un esame delle relazioni tra le vulnerabilità e le misure di sicurezza esistenti per determinare le aree di maggiore rischio.

- **Determinazione dell'Impatto**: Studio degli effetti potenziali delle minacce identificate, valutando impatti su diversi livelli, come operativi, legali e di reputazione. Questi impatti saranno discussi in termini di severità e del loro effetto a lungo termine sulle operazioni di Alpha Healthcare.

- **Stima della Probabilità**: Valutazione della frequenza e delle condizioni sotto cui una minaccia potrebbe manifestarsi, basata su analisi di tendenze di settore e dati storici interni.

3 - Conduzione della Valutazione - STEP 2

La seconda fase del processo di valutazione del rischio consiste nell'esecuzione della valutazione. L'obiettivo di questa fase è produrre un elenco di rischi per la sicurezza delle informazioni che possa essere classificato in base al livello di rischio e utilizzato per informare le decisioni di risposta al rischio. Per raggiungere questo obiettivo, analizzeremo le minacce e le vulnerabilità, gli impatti e la probabilità, nonché l'incertezza associata al processo di valutazione del rischio. Questa fase comprende anche la raccolta di informazioni essenziali come parte di ogni compito ed è condotta in conformità con il contesto di valutazione stabilito nella fase di preparazione del processo di valutazione del rischio. L'aspettativa per le valutazioni del rischio è quella di coprire adeguatamente l'intero spazio delle minacce in conformità con le definizioni specifiche, le linee guida e le indicazioni stabilite durante la fase Prepare. Tuttavia, nella pratica, una copertura adeguata nell'ambito delle risorse disponibili può richiedere la generalizzazione delle fonti di minaccia, degli eventi di minaccia e delle vulnerabilità per garantire una copertura completa e la valutazione di fonti, eventi e vulnerabilità specifici e dettagliati solo se necessario per raggiungere gli obiettivi della valutazione del rischio.

Nella fase che segue, utilizzeremo unicamente le tabelle del NIST SP 800-30, per una questione di facilità di lettura, data la complessità dell’argomento.

3.1 Identificazione delle Fonti di Minaccia e degli Eventi (Appendix D)

In questa fase identificheremo e caratterizzeremo le fonti di minaccia che destano preoccupazione, comprese le caratteristiche di capacità, intento e obiettivo per le minacce avversarie.

Summary of Key Activities – Task 2-1

- Identify threat source inputs (see **Table D-1**, as tailored by the organization).
- Identify threat sources (see **Table D-2**, as tailored by the organization).
- Determine if threat sources are relevant to the organization and in scope (see **Table D-1**, as tailored by the organization).
- Create or update the assessment of threat sources (see **Table D-7** for adversarial threat sources and **Table D-8** for non-adversarial threat sources, as tailored by the organization).
  - For relevant adversarial threat sources:
    - Assess adversary capability (see **Table D-3**, as tailored by the organization).
    - Assess adversary intent (see **Table D-4**, as tailored by the organization).
    - Assess adversary targeting (see **Table D-5**, as tailored by the organization).
  - For relevant non-adversarial threat sources:
    - Assess the range of effects from threat sources (see **Table D-6**, as tailored by the organization).

TABELLA D-7 IDENTIFICAZIONE DELLE FONTI DI MINACCIA AVVERSARIA

Identifier	Threat Source	In Scope	Capability	Intent	Targeting
D-7-1	Gruppo che sta cercando di sfruttare la dipendenza dell'organizzazione dalle risorse informatiche	Si	Alto	Alto	Molto alto

3.2 - Identificazione degli eventi di minaccia (APPENDIX E)

Summary of Key Activities – Task 2-2

- Identify threat event inputs (see **Table E-1**, as tailored by the organization).
- Identify threat events (see **Table E-2** for adversarial threat events and **Table E-3** for non-adversarial threat events, as tailored by the organization); create or update **Table E-5**.
- Identify threat sources that could initiate the threat events (see **Table D-7** and **Table D-8**, as tailored by the organization); update **Table E-5**.
- Assess the relevance of threat events to the organization (see **Table E-4**, as tailored by the organization); update **Table E-5**.
- Update Columns 1-6 in **Table I-5** for adversarial risk (see **Table E-5** and **Table D-7**); or update Columns 1-4 in **Table I-7** for non-adversarial risk (see **Table E-5** and **Table D-8**).

TABELLA E-5 IDENTIFICAZIONE EVENTI DI MINACCIA

Identifier	Threat Event	Threat Source	Relevance
E-5-1	Craft Phishing Attack	Vedi tabella D-7	Confermato

3.3 - Identificazione delle vulnerabilità e delle condizioni predisponenti

Summary of Key Activities – Task 2-3

- Identify vulnerability and predisposing condition inputs (see **Table F-1**, as tailored by the organization).
- Identify vulnerabilities using organization-defined information sources; create or update **Table F-3**.
- Assess the severity of identified vulnerabilities (see **Table F-2**, as tailored by the organization); update **Table F-3**.
- Identify predisposing conditions (see **Table F-4**, as tailored by the organization); create or update **Table F-6**.
- Assess the pervasiveness of predisposing conditions (see **Table F-5**, as tailored by the organization); update **Table F-6**.
- Update Column 8 in **Table I-5** for adversarial risk; or update Column 6 in **Table I-7** for non-adversarial risk (see **Table F-3** and **Table F-6**).
- Update Column 9 in **Table I-5** for adversarial risk; or update Column 7 in **Table I-7** for non-adversarial risk (see **Table F-2** and **Table F-5**).

TABELLA F-3 IDENTIFICAZIONE DELLE VULNERABILITÀ

Identifier	Vulnerability	Vulnerability Severity
F-3-1	Personale non aggiornato su pratiche di sicurezza informatica	Moderato
F-3-2	Mancanza MFA	Alto
F-3-3	Sistemi IT non aggiornati	Alto

TABELLA F-6 IDENTIFICAZIONE CONDIZIONI PREDISPONENTI

Identifier	Predisposing Condition	Pervasiveness of condition
F-6-1	IFORMATION	Alto
F-6-2	TECHNICAL	Alto
F-6-3	TECHNICAL	Alto

3.4 - Determinazione dell'impatto

Summary of Key Activities – Task 2-5

- Identify impact determination inputs (see **Table H-1** as tailored by the organization).
- Identify impact determination factors using organization-defined information sources.
- Identify adverse impacts and affected assets (see **Table H-2**, as tailored by the organization); create or update **Table H-4**.
- Assess the maximum impact associated with the affected assets (see **Table H-3**, as tailored by the organization); update **Table H-4**.
- Update Column 12 in **Table I-5** for adversarial risk; or update Column 10 in **Table I-7** for non-adversarial risk.

TABELLA H-4 IDENTIFICAZIONE IMPATTO AVVERSO

Type of impact	Impact	Maximum Impact
H-2	Danneggiamento o perdita di beni informativi	Alto

3.5 - Determinazione rischio

Threat Event	Threat Source	Capability	Intent	Targeting	Relevance	Likehood of Attack Initiation	Vilnerabilities and predisposing condition	Severity and Pervasivness	Likehood Initiated Attack Success	Overall Likehood	Levell of Impact	Risk
E-5-1	D-7-1	ALTO	ALTO	MOLTO ALTO	CONFERMATO	MOLTO ALTO	F-3-1	MODERATO	ALTO	MOLTO ALTO	ALTO	ALTO
E-5-1	D-7-1	ALTO	ALTO	MOLTO ALTO	CONFERMATO	MOLTO ALTO	F-3-2	ALTO	ALTO	MOLTO ALTO	ALTO	ALTO
E-5-1	D-7-1	ALTO	ALTO	MOLTO ALTO	CONFERMATO	MOLTO ALTO	F-3-3	ALTO	ALTO	MOLTO ALTO	ALTO	ALTO

L’azienda può accettare solo un rischio di livello bassa vista l’importanza dell’asset in esame, procederemo quindi al miglioramento dei controlli per riportare il rischio entro il livello accettabile. Successivamente andrà effettuato un’altra fase di Risk Assestment per valutare che i controlli abbiano avuto effetto.