REPORT DI RISK ASSESSMENT PER L'AZIENDA ALPHA

Data 08/05/2024

INDICE

Introduzione

Questo report presenta il processo di Risk Assessment per l'Azienda Alpha, un fornitore leader di servizi sanitari online che gestisce un'ampia infrastruttura IT. L'obiettivo del Risk Assessment è identificare e valutare i rischi associati alle minacce attuali e potenziali per l'azienda, consentendo la pianificazione e l'implementazione di misure di mitigazione appropriate.

Per lo sviluppo di questo RA vengono presi in considerazione solo gli STEP 1 e 2 del processo di valutazione del rischio proposto dalla normativa NIST SP800-30r.

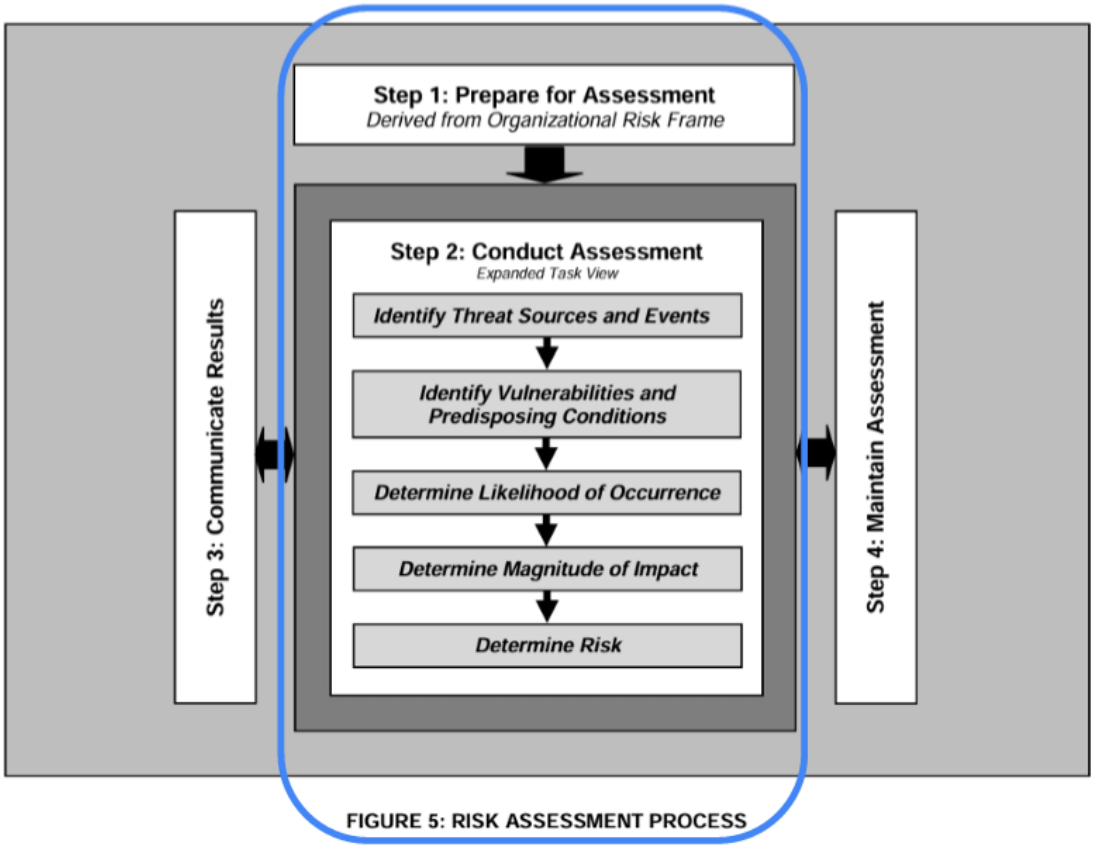

FIGURE 5: RISK ASSESSMENT PROCESS

Step 1: Preparazione

In questa fase, l'obiettivo è comprendere il contesto dell'organizzazione, identificare le risorse critiche e stabilire il contesto operativo per il Risk Assessment. Considerando l'azienda Alpha, si raccoglieranno informazioni sulle sue attività, infrastrutture, asset critici e minacce note.

Per sviluppare l'RA di questo scenario viene fatto riferimento alla normativa del NIST SP800-30r. Le tabelle prese in considerazione per l'analisi sono: E-5, F-3, F-6, H-4, I-5.

Scopo del RA: Valutare e mitigare i rischi associati alle minacce esterne in fase di ricognizione che potrebbero compromettere la sicurezza dell'infrastruttura IT dell'Azienda Alpha e la riservatezza dei dati sanitari dei pazienti.

Ambito del RA: Limitato alle attività di ricognizione esterna eseguite da un gruppo criminale organizzato, inclusi scanning, sniffing, OSINT e sorveglianza, che mirano a esfiltrare informazioni sanitarie per rivenderle. Il focus sarà sull'infrastruttura IT dell'Azienda Alpha, escludendo le minacce interne e altri tipi di attacchi.

Ipotesi: Si ipotizza che il gruppo criminale organizzato abbia le risorse e le capacità per eseguire attacchi coordinati contro l'Azienda Alpha con l'obiettivo specifico di esfiltrare e rivendere le informazioni sanitarie dei pazienti.

Vincoli:

- L'organizzazione non ha abilitato l'autenticazione multifattore (MFA) e non esegue regolarmente attività di Vulnerability Assessment.
- L'analisi sarà concentrata solo sugli impatti delle minacce esterne in fase di ricognizione sulla sicurezza e sulla riservatezza dei dati, tralasciando altri scenari di minaccia e rischi associati.

Tabella D-7: Contesto Operativo

Identificatore	Fonte della Minaccia	Fonte di Informazioni	In Portata	Capacità	Intento	Targeting
Tabella D-2 e Task 1-4	Gruppo Criminale Organizzato	OSINT, Sorveglianza, Scanning, Sniffing	Sì	Alta	Moderato: Esfiltrare informazioni sanitarie per rivenderle	Alto

Step 2: Identificazione delle Minacce

In questa fase, identifichiamo e analizziamo le minacce potenziali che potrebbero sfruttare le vulnerabilità dell'azienda. Si considerano i metodi utilizzati dalle minacce per eseguire la ricognizione esterna, come scanning, sniffing, OSINT, sorveglianza e possibili conseguenze.

Tabella E-5: Identificazione delle Minacce

Identificatore	Fonte di Informazioni sull'Evento di Minaccia	Fonte della Minaccia	Pertinenza
Metodi di ricognizione	Eseguire la ricognizione/analisi della rete perimetrale.	Gruppo criminale organizzato	**Confermato**
Metodi di Ricognizione	Eseguire lo sniffing di rete delle reti esposte.	Gruppo criminale organizzato	**Confermato**
Metodi di ricognizione	Raccogliere informazioni utilizzando l'individuazione open source delle informazioni dell'organizzazione.	Gruppo criminale organizzato	**Confermato**
Ottenere informazioni	Ottenere informazioni riservate tramite lo sniffing di rete di reti esterne.	Gruppo criminale organizzato	**Previsto**
Ottenere informazioni	Ottenere informazioni sensibili tramite esfiltrazione.	Gruppo criminale organizzato	**Previsto**

Tabella F-3: Vulnerabilità

Identificatore	Fonte di Informazioni sulla Vulnerabilità	Gravità della Vulnerabilità
Autenticazione non autorizzata	Rapporti di valutazione della sicurezza	**Molto Alto** Il controllo di sicurezza pertinente o altre correzioni non è implementato e non pianificato;
Vulnerabilità del sistema informativo non rilevate	Rapporti di valutazione della sicurezza	**Molto Alto** Il controllo di sicurezza pertinente o altre correzioni non è implementato e non pianificato;

Tabella F-6: Valutazione delle condizioni predisponenti

Identificatore	Condizione Predisponente	Pervasività della Condizione
Autenticazione non autorizzata	Mancata abilitazione dell'autenticazione multifattore (MFA)	Alta
Vulnerabilità del sistema informativo non rilevate	Mancata esecuzione regolare delle attività di Vulnerability Assessment	Alta

Tabella H-4: Impatto

Tipo di Impatto	Impatto sull'Asset Interessato	Impatto Massimo
Danno a operazioni	Danni (ad esempio, costi finanziari, sanzioni) dovuti alla non conformità.	Alto
Danno a operazioni	Danni all'immagine o alla reputazione	Alto

Tipo di Impatto	Impatto sull'Asset Interessato	Impatto Massimo
Danno a operazioni	Danneggiamento o perdita di risorse informative.	**Alto**
Danno a persone	Perdita di informazioni di identificazione personale.	**Molto alto**

Tabella I-5: Impatto delle Vulnerabilità

L'Appendice I della normativa NIST SP800-30R fornisce un modello dettagliato per la valutazione del rischio.

Questo modello è progettato per guidare gli analisti attraverso una serie strutturata di passaggi per identificare, analizzare e valutare i rischi in un determinato contesto operativo. Il modello si basa su una serie di elementi chiave, tra cui la descrizione degli eventi minacciosi, le fonti delle minacce, le caratteristiche delle fonti delle minacce, la rilevanza delle minacce, la probabilità di iniziazione dell'attacco, le vulnerabilità e le condizioni predisponenti, la gravità e la pervasività delle minacce, la probabilità di successo dell'attacco iniziato, la probabilità complessiva e il livello di impatto.

Questo approccio strutturato consente di avere una valutazione completa e dettagliata del rischio prendendo in considerazione le valutazioni ottenute con l’applicazione delle tabelle precedenti, consentendo all’organizzazione di comprendere meglio le minacce e di adottare misure di mitigazione appropriate per proteggere i loro asset critici.

Tabella I-5: Impatto delle Vulnerabilità

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	Rischio
		Capacità	Intento	Target								
Esfiltrazione dati sensibili	Gruppo Criminale Organizzato	Alta	**Moderato**	Alto	Alta	Alta	Mancata abilitazione di MFA, Mancata esecuzione regolare delle valutazioni delle vulnerabilità	Alto	Molto alta	Alta	Alto	Alto

Considerazioni sullo standard HIPAA

Nel contesto del Risk Assessment per l'Azienda Alpha, è importante considerare anche le disposizioni di HIPAA (Health Insurance Portability and Accountability Act) relative alla protezione dei dati sanitari dei pazienti. Sebbene HIPAA non menzioni specificamente l'OSINT o la ricerca di informazioni da parte di minacce esterne, stabilisce standard e requisiti generali per la protezione dei dati sanitari.

Protezione dei Dati Sanitari: HIPAA richiede che gli enti sanitari proteggano i dati sanitari dei pazienti da accessi non autorizzati e da usi impropriati. Ciò implica l'adozione di misure di sicurezza tecniche, amministrative e fisiche per prevenire l'accesso non autorizzato ai dati, indipendentemente dalla fonte.

Sicurezza delle Informazioni: HIPAA richiede anche che gli enti sanitari implementino misure adeguate a garantire la sicurezza delle informazioni sanitarie, inclusa la protezione dai rischi derivanti da minacce esterne come l'OSINT. Questo potrebbe includere l'adozione di politiche e procedure per monitorare e mitigare i rischi derivanti dalla ricerca di informazioni da parte di minacce esterne che potrebbero compromettere la riservatezza dei dati sanitari.

Risposta alle Violazioni: HIPAA richiede agli enti sanitari di sviluppare e implementare piani di risposta alle violazioni dei dati per affrontare e mitigare le conseguenze delle violazioni della sicurezza dei dati. Questi piani potrebbero includere procedure per affrontare le minacce esterne, come la ricerca di informazioni da parte di attori malevoli, che potrebbero portare a violazioni della sicurezza dei dati sanitari.

Integrare queste considerazioni su HIPAA nel processo di Risk Assessment aiuterà l'Azienda Alpha a comprendere e gestire in modo efficace i rischi associati alla gestione dei dati sanitari sensibili dei pazienti, contribuendo alla protezione della privacy e alla conformità normativa.

Valutazioni e Raccomandazioni

Dato che l'organizzazione accetta solamente un rischio basso per tutti gli eventi di rischio identificati, inclusi quelli legati al valore critico dei dati sanitari, è necessario elaborare strategie mirate per ridurre il livello di rischio attuale a un livello accettabile.

Valutazione Attuale del Rischio:

- **Rischi Identificati:** Sono stati identificati rischi legati alla mancanza di autenticazione multifattore (MFA), alla mancata esecuzione regolare delle valutazioni delle vulnerabilità e alle minacce esterne di ricognizione.

- **Livello Attuale del Rischio:** Il livello attuale del rischio è considerato alto, poiché la combinazione di vulnerabilità e minacce potrebbe compromettere gravemente la sicurezza dei dati sanitari sensibili.

Ipotesi per Ridurre il Rischio:

1. **Implementazione di MFA:** Una delle prime azioni da intraprendere è l'implementazione dell'autenticazione multifattore (MFA) per l'accesso ai sistemi e ai dati sensibili. Questo ridurrà significativamente il rischio di accesso non autorizzato e di compromissione dei dati.

2. **Esecuzione di Valutazioni delle Vulnerabilità Regolari:** È essenziale avviare un programma regolare di valutazione delle vulnerabilità per identificare e mitigare le potenziali debolezze nei sistemi e nelle infrastrutture IT. Ciò contribuirà a ridurre la superficie di attacco e a prevenire exploit da parte di minacce esterne.

3. **Miglioramento delle Difese contro le Minacce Esterne:** Potrebbe essere necessario rafforzare le difese contro le minacce esterne, ad esempio tramite l'aggiornamento delle firme dei firewall, l'implementazione di sistemi di rilevamento delle intrusioni avanzati e la collaborazione con fornitori di servizi di sicurezza gestiti per monitorare e rispondere alle minacce in tempo reale.

Prossimi Passaggi:

1. **Pianificazione e Implementazione delle Misure di Sicurezza:** Definire un piano dettagliato per implementare le misure di sicurezza identificate, inclusa una pianificazione temporale e una suddivisione delle responsabilità tra i team interni e, se necessario, i fornitori esterni.

2. **Monitoraggio e Valutazione Continua:** Dopo l'implementazione delle misure di sicurezza, è essenziale monitorare costantemente l'efficacia delle stesse e valutare periodicamente il livello di rischio per garantire il mantenimento di un livello accettabile di sicurezza dei dati sanitari.

3. **Formazione del Personale:** Fornire formazione regolare al personale sull'importanza della sicurezza delle informazioni e sulle procedure da seguire per mantenere un ambiente sicuro. Il coinvolgimento del personale è fondamentale per garantire la conformità e la consapevolezza dei rischi.

Seguendo questi passaggi, l'Azienda Alpha può ridurre efficacemente il livello di rischio attuale a un livello accettabile, garantendo al contempo la sicurezza e la riservatezza dei dati sanitari dei pazienti in conformità con gli standard HIPAA e le migliori pratiche di sicurezza informatica.