

RISK MANAGEMENT

ANALISI DEL RISCHIO


MARIA HUAPAYA





INDICE

- Traccia (pag 3)

 - 1. Introduzione (pag 4)
 - Scopo del report
 - Metodologia utilizzata
 - 2. Presentazione dell'azienda di servizi cloud (pag 5)
 - Panoramica dell'azienda
 - Struttura e servizi offerti
 - 3. Descrizione del rischio di violazione dei dati (pag 6)
 - Tipologie di dati gestiti
 - Potenziali vulnerabilità
 - 4. Vulnerabilità nel software e nelle configurazioni di sicurezza (pag 7)
 - Vulnerabilità del software
 - Vulnerabilità delle configurazioni di sicurezza
 - 5. Analisi del Rischio (pag 8)
 - Stima della probabilità di un incidente
 - Discussione sulle potenziali perdite finanziarie
 - Stima del costo di una singola violazione dei dati
 - Previsione della frequenza degli incidenti
 - 6. Analisi del Rischio Semi-Quantitativa (pag 9)
 - Descrizione del processo semplificato per l'analisi del rischio
 - Utilizzo delle tabelle G-4/H-3/I-2 del NIST SP 800-30 Rev. 1
 - Calcolo del rischio basato sul fatturato annuale dell'azienda
 - Integrazione dei valori delle tabelle NIST nella valutazione complessiva
 - 7. Conclusioni (pag 12)
 - Riassunto dei risultati dell'analisi
 - Raccomandazioni per future analisi del rischio
- 



TRACCIA

Un'azienda di servizi cloud è esposta al rischio di violazione dei dati a causa di vulnerabilità nel software e nelle configurazioni di sicurezza.

L'azienda stima che la probabilità di un incidente di questo tipo sia del 70%.

Una violazione dei dati potrebbe portare a perdite finanziarie dovute a sanzioni normative, risarcimenti ai clienti e danni reputazionali.

Sulla base delle stime, una singola violazione dei dati potrebbe costare all'azienda circa 5 milioni di euro. Inoltre, l'azienda prevede che un incidente simile possa verificarsi in media due volte all'anno.

Il fatturato annuale dell'azienda è di 200 milioni di euro.

Svolgere un'analisi del rischio semi-quantitativa, utilizzando il processo semplificato visto a lezione, tabelle G-4/H-3/I-2 NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments,

<https://csrc.nist.gov/pubs/sp/800/30/r1/final>

Creare un report in cui descrivere i passaggi svolti per l'analisi.



INTRODUZIONE

Scopo del Report

Il presente report è stato redatto con l'obiettivo di valutare i rischi associati a potenziali violazioni dei dati per una società di servizi cloud. Attraverso l'analisi dei rischi, miriamo a identificare le vulnerabilità principali che potrebbero portare a perdite finanziarie, danni reputazionali e sanzioni normative. Il report illustrerà anche le misure di mitigazione del rischio da considerare per ridurre la probabilità e l'impatto di tali incidenti.

Metodologia Utilizzata

Per l'analisi del rischio, è stato adottato un approccio semi-quantitativo seguendo le linee guida del NIST SP 800-30 Rev. 1. Questo metodo combina elementi quantitativi e qualitativi, permettendo una stima più precisa del rischio basata su probabilità di eventi e potenziali impatti finanziari. Sono state utilizzate le tabelle G-4, H-3 e I-2 per classificare e valutare i rischi in maniera strutturata e sistematica. L'analisi è stata eseguita considerando sia la probabilità di occorrenza degli incidenti di sicurezza sia il loro impatto finanziario sull'organizzazione.

PRESENTAZIONE DELL'AZIENDA DI SERVIZI CLOUD

Panoramica dell'azienda

CloudSecure Solutions è un fornitore leader di servizi cloud che offre soluzioni integrate di storage, elaborazione e rete a clienti in settori ad alta responsabilità come finanziario, sanità e agenzie governative.

CloudSecure ha costantemente ampliato la propria gamma di servizi per supportare l'innovazione digitale e migliorare l'efficienza operativa dei suoi clienti.

Con un fatturato annuale di 200 milioni di euro e una presenza globale, CloudSecure è riconosciuta per la sua affidabilità e innovazione nel campo dei servizi cloud.

Struttura e servizi offerti

L'azienda è strutturata per garantire l'alta disponibilità e la sicurezza dei dati, con data center distribuiti in più località geografiche per assicurare continuità operativa e resilienza. I servizi offerti includono:

- Cloud Storage: soluzioni sicure per l'archiviazione dati che permettono ai clienti di scalare le risorse secondo necessità.
- Cloud Computing: piattaforme di elaborazione che offrono capacità computazionale flessibile e scalabile.
- Networking: servizi di connettività di rete che assicurano prestazioni ottimali e sicurezza dei dati trasmessi.
- Servizi di sicurezza: protezione completa dei dati con crittazione, firewall avanzati e altre tecnologie di sicurezza.

Questi servizi sono supportati da un robusto quadro di governance del rischio, essenziale per mitigare le potenziali minacce alla sicurezza dei dati e per garantire la compliance con le normative vigenti.

DESCRIZIONE DEL RISCHIO DI VIOLAZIONE DEI DATI

Tipologie di dati gestiti

CloudSecure gestisce una vasta gamma di dati sensibili e critici per l'operatività dei suoi clienti.

Questi includono dati personali, informazioni finanziarie, record sanitari e dati governativi.

La natura sensibile di tali dati rende l'azienda un target attraente per gli attacchi informatici, con implicazioni legali e finanziarie significative in caso di violazione.

Potenziali vulnerabilità

Il rischio di violazione dei dati può derivare da diverse fonti, tra cui:

- Intrusioni esterne: attacchi mirati da parte di cybercriminali che sfruttano vulnerabilità nel software o nelle configurazioni di sicurezza.
- Errori umani: errori di configurazione o di gestione dei dati da parte dei dipendenti che possono portare a esposizioni accidentali o a violazioni di sicurezza.
- Software obsoleto: l'utilizzo di software non aggiornato può contenere vulnerabilità conosciute che facilitano gli attacchi informatici.
- Phishing e altre tecniche di ingegneria sociale: attacchi che mirano a ingannare i dipendenti per ottenere credenziali di accesso o informazioni riservate.

La combinazione di questi fattori aumenta significativamente la probabilità di incidenti di sicurezza, con il potenziale di compromettere la reputazione di CloudSecure e di causare gravi perdite finanziarie e sanzioni normative.

VULNERABILITÀ NEL SOFTWARE E NELLE CONFIGURAZIONI DI SICUREZZA

Vulnerabilità del software

Le vulnerabilità del software rappresentano una delle principali minacce per la sicurezza informatica. CloudSecure, ad esempio, deve affrontare una serie di rischi. Uno di questi è rappresentato dalle vulnerabilità non patchate. Questo accade quando le patch di sicurezza non vengono applicate in tempo, lasciando i sistemi vulnerabili a exploit noti. Un altro rischio proviene dall'uso di software di terze parti, che può introdurre incertezze, soprattutto se il software non viene regolarmente aggiornato o monitorato. Infine, gli errori di configurazione, dovuti a configurazioni improprie o complesse, possono aumentare il rischio di esposizione, rendendo difficile la gestione e il monitoraggio efficace.

Vulnerabilità delle configurazioni di sicurezza

Configurazioni di sicurezza inadeguate rappresentano un fattore critico di rischio. Ad esempio, configurazioni di rete non sicure, come l'insufficiente segmentazione della rete e le politiche di accesso inadeguate, possono permettere agli attaccanti di muoversi lateralmente all'interno della rete una volta guadagnato l'accesso. Le politiche di sicurezza deboli, come l'uso di password deboli o l'assenza di autenticazione multifattore, rendono più facile per gli aggressori accedere a sistemi sensibili. Infine, la mancanza di procedure regolari di audit e monitoraggio può far sì che alcune vulnerabilità rimangano non rilevate e non gestite per lunghi periodi.

ANALISI DEL RISCHIO

Stima della probabilità di un incidente

Secondo le valutazioni interne e le analisi di scenario, la probabilità che si verifichi una violazione dei dati presso CloudSecure è stimata al 70%. Questa stima si basa su fattori quali le vulnerabilità esistenti nel software e nelle configurazioni, nonché su recenti tendenze e attacchi nel settore dei servizi cloud.

Discussione sulle potenziali perdite finanziarie

Una violazione dei dati potrebbe esporre CloudSecure a significative perdite finanziarie:

- Sanzioni normative: le violazioni dei dati possono portare a multe e sanzioni da parte di enti regolatori, specialmente in settori altamente regolamentati come la sanità e i servizi finanziari.
- Risarcimenti ai clienti: l'azienda potrebbe essere tenuta a risarcire i clienti per le perdite subite a causa della violazione dei dati.
- Danni reputazionali: la fiducia dei clienti è cruciale per un fornitore di servizi cloud; una violazione potrebbe danneggiare gravemente la reputazione di CloudSecure, con un impatto a lungo termine sui futuri ricavi.

Stima del costo di una singola violazione dei dati

Sulla base di stime interne, una singola violazione dei dati potrebbe costare a CloudSecure circa 5 milioni di euro. Questa cifra include le sanzioni, i risarcimenti ai clienti, e le spese per le attività di recupero e rafforzamento della sicurezza post-violazione.

Previsione della frequenza degli incidenti

È previsto che un incidente di violazione dei dati possa verificarsi mediamente due volte all'anno, basandosi sulle tendenze attuali e sulla valutazione del contesto di sicurezza di CloudSecure.

ANALISI DEL RISCHIO SEMI-QUANTITATIVA

Descrizione del processo semplificato per l'analisi del rischio semi-quantitativa

L'analisi del rischio semi-quantitativa adottata da CloudSecure combina elementi qualitativi e quantitativi per fornire una stima più precisa del rischio. Questo processo inizia con la raccolta di dati relativi agli incidenti passati e alle tendenze del settore, integrando queste informazioni con le valutazioni qualitative delle vulnerabilità e degli impatti potenziali. Si utilizzano poi scale semi-quantitative, come quelle fornite dalle tabelle G-4/H-3/I-2 del NIST SP 800-30 Rev. 1, per assegnare valori numerici agli impatti e alle probabilità.

Utilizzo delle tabelle G-4/H-3/I-2 del NIST SP 800-30 Rev. 1

Queste tabelle aiutano a categorizzare e valutare i rischi in modo strutturato:

- tabella G-4: viene utilizzata per valutare la verosomiglianza di un evento rischioso basandosi su dati storici e scenari ipotetici.
- tabella H-3: aiuta a determinare l'impatto finanziario di una violazione dei dati, considerando vari fattori come perdite dirette, sanzioni e danni reputazionali.
- tabella I-2: utilizzata per combinare le informazioni di probabilità e impatto per arrivare a una valutazione complessiva del rischio.

Calcolo del rischio basato sul fatturato annuale dell'azienda

Per effettuare un'analisi dettagliata del rischio finanziario derivante da violazioni dei dati, consideriamo diversi fattori essenziali che influenzano direttamente il bilancio di CloudSecure. La procedura adottata per il calcolo del rischio semi-quantitativo include i seguenti passaggi:

- Valutazione del Costo di una Singola Violazione: basandoci su analisi interne, stime di settore e incidenti passati, stimiamo che il costo diretto e indiretto di una singola violazione dei dati per CloudSecure sia di circa 5 milioni di euro. Questo valore include componenti come:
 - Sanzioni normative e multe.
 - Risarcimenti dovuti ai clienti per la compromissione dei loro dati.

- Costi operativi legati alla gestione dell'incidente e alla comunicazione di crisi.
- Spese per la revisione e il rafforzamento delle infrastrutture di sicurezza post-incidente.
- Frequenza degli Incidenti: dalle analisi di rischio basate su dati storici e sul monitoraggio corrente delle minacce, CloudSecure stima che potrebbero verificarsi due significative violazioni dei dati all'anno. Questo tasso di occorrenza è calcolato tenendo conto di variabili come il panorama delle minacce attuali, l'efficacia delle misure di sicurezza in atto e le tendenze osservate nel settore dei servizi cloud.
- Per determinare l'Annual Loss Expectancy (ALE) identifico quindi i due componenti chiave: la Single Loss Expectancy (SLE) e l'Annualized Rate of Occurrence (ARO)
 1. **Single Loss Expectancy (SLE):** rappresenta il costo stimato che l'azienda si aspetta di sostenere in caso di un singolo evento di violazione dei dati. Questa valutazione include le perdite dirette come danni e furto di risorse, costi operativi per il ripristino dei sistemi e qualsiasi impatto indiretto come la perdita di business o sanzioni. Per CloudSecure, l'SLE è stato valutato in 5 milioni di euro, basato sul costo stimato di una violazione dei dati, incluse le conseguenze e le responsabilità ad essa associate.
 2. **Annualized Rate of Occurrence (ARO):** è una stima del numero di volte che ci si aspetta che un evento di rischio si verifichi in un anno. L'ARO è basato sull'analisi dei dati storici degli incidenti e sul contesto attuale delle minacce. Per CloudSecure, con una probabilità del 70% che si verifichi un incidente di questo tipo, e considerando le informazioni attuali, l'ARO è stato stimato in 2, riflettendo la previsione che tali incidenti possano verificarsi due volte all'anno.
 3. **Annual Loss Expectancy (ALE):** è il valore atteso di perdita per l'azienda in un anno a causa di eventi di rischio. L'ALE si ottiene moltiplicando la SLE per l'ARO:
 $ALE = SLE \times ARO$
 $ALE = 5 \text{ milioni di euro} \times 2 = 10 \text{ milioni di euro}$

Con un fatturato annuale di 200 milioni di euro, l'ALE di 10 milioni di euro rappresenta circa il 5% del fatturato totale.

Integrazione dei valori delle tabelle NIST nella valutazione complessiva

Selezione della verosomiglianza: al valore semi-quantitativo del 70% corrisponde il valore "Moderate" della tabella G-4 del NIST SP 800-30 Rev. 1.

TABLE G-4: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT RESULTING IN ADVERSE IMPACTS

| Qualitative Values | Semi-Quantitative Values | | Description |
|--------------------|--------------------------|----|---|
| Very High | 96-100 | 10 | If the threat event is initiated or occurs, it is almost certain to have adverse impacts. |
| High | 80-95 | 8 | If the threat event is initiated or occurs, it is highly likely to have adverse impacts. |
| Moderate | 21-79 | 5 | If the threat event is initiated or occurs, it is somewhat likely to have adverse impacts. |
| Low | 5-20 | 2 | If the threat event is initiated or occurs, it is unlikely to have adverse impacts. |
| Very Low | 0-4 | 0 | If the threat event is initiated or occurs, it is highly unlikely to have adverse impacts. |

Selezione dell'impatto: al valore semi-quantitativo del 5% corrisponde il valore "Low" della tabella H-3 del NIST SP 800-30 Rev. 1

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. |
| 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. |
| Low | 5-20 | 2 | The threat event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a 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 noticeably reduced; (ii) result in minor damage to organizational assets; (ii) result in minor financial loss; or (iv) result in minor harm to individuals. |
| Very Low | 0-4 | 0 | The threat event could be expected to have a negligible adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. |

Livello di rischio complessivo: Combinando la verosomiglianza "Moderate" e l'impatto "Low" è possibile valutare che il rischio complessivo per CloudSecure è classificato con il valore "Low" della tabella I-2 del NIST SP 800-30 Rev. 1

TABLE I-2: ASSESSMENT SCALE – LEVEL OF RISK (COMBINATION OF LIKELIHOOD AND IMPACT)

| Likelihood (Threat Event Occurs and Results in Adverse Impact) | Level of Impact | | | | |
|---|-----------------|------------|----------|----------|-----------|
| | Very Low | Low | Moderate | High | Very High |
| Very High | Very Low | Low | Moderate | High | Very High |
| High | Very Low | Low | Moderate | High | Very High |
| Moderate | Very Low | Low | Moderate | Moderate | High |
| Low | Very Low | Low | Low | Low | Moderate |
| Very Low | Very Low | Very Low | Very Low | Low | Low |



CONCLUSIONI

Riassunto dei risultati dell'analisi

L'analisi semi-quantitativa del rischio condotta per CloudSecure ha evidenziato che le violazioni dei dati rappresentano una minaccia significativa per l'azienda, con un Annual Loss Expectancy (ALE) stimato di 10 milioni di euro all'anno. Questo equivale a circa il 5% del fatturato annuale, sottolineando l'importanza di una gestione efficace del rischio per proteggere non solo le risorse finanziarie ma anche la reputazione aziendale.

Le principali vulnerabilità identificate includono software non aggiornato, configurazioni di sicurezza inadeguate e minacce interne potenziali.

Raccomandazioni per future analisi del rischio

Per continuare a proteggere l'azienda dalle minacce emergenti, si raccomanda di:

- Aggiornare regolarmente le politiche di sicurezza e le infrastrutture tecnologiche per rispondere alle nuove vulnerabilità man mano che vengono identificate.
- Incrementare la formazione e la consapevolezza sulla sicurezza per tutti i dipendenti per minimizzare il rischio di errori umani e aumentare la resilienza contro attacchi di ingegneria sociale.
- Effettuare valutazioni di rischio periodiche, adattando le strategie di mitigazione in base all'evoluzione del panorama delle minacce e alle modifiche nel modello di business di CloudSecure.
- Esplorare soluzioni di assicurazione cyber per gestire meglio le conseguenze finanziarie delle violazioni dei dati.

GRAZIE

MARIA HUAPAYA

