EPICODE

S1L4

Analisi del rischio

26 aprile 2024

Team:

- Davide Di Turo
- Manuel Di Gangi
- Marco Fasani
- Oliviero Camarota

INDICE

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.

Per svolgere un'analisi del rischio semi-quantitativa, si possono eseguire i passaggi generali del processo e usufruire delle tabelle fornite dal NIST SP 800-30 Rev 1 come indicato dall'esercizio.

1. Analisi del contesto

Quando si affronta un'analisi del rischio semi-quantitativa, è essenziale comprendere tutti gli elementi coinvolti. In questo caso, stiamo valutando il rischio di violazione dei dati per un'azienda di servizi cloud.

1.1 Analisi degli asset

Gli asset principali sono i dati sensibili dei clienti e la reputazione dell'azienda. La perdita o la compromissione di questi asset potrebbero avere gravi conseguenze finanziarie e reputazionali.

1.1.1 Identificazione degli asset critici:

- Dati clienti (informazioni personali,finanziarie ecc)
- Servizi cloud (server, rete, archiviazione)
- Software o piattaforme utilizzate
- Fiducia o reputazione dei clienti dell'azienda

1.1.2 Valutazione del valore degli asset:

- Dati clienti: Sono di un'importanza elevatissima in termini di riservatezza e integrità. Valore: *Elevato*
- Servizi Cloud: è necessaria per assegnare i servizi ai clienti. Valore: *Elevato*
- Software o piattaforme utilizzate: Critici per garantire la qualità della sicurezza dei servizi. Valore: *Elevato*
- Fiducia o reputazione dei clienti dell'azienda: Di totale importanza per il successo dell'azienda in ottica futura. Valore: *Elevato*

  Considerando il valore degli asset critici, è evidente che la protezione dei dati e la sicurezza dell'infrastruttura e dei servizi cloud devono essere prioritari. Le potenziali

perdite finanziarie associate alla violazione dei dati non riguardano solo costo in termini monetari, ma anche la reputazione aziendale e alla fiducia dei clienti.

1.2 Analisi delle minacce

La minaccia principale è rappresentata dalle violazioni dei dati, che potrebbe derivare da vulnerabilità nel software utilizzato dall'azienda o da configurazioni di sicurezza non ottimali

1.2.1 Identificazione delle minacce

Violazione dei dati:

- Vulnerabilità nella sicurezza dei software o web-app utilizzati potrebbero essere sfruttate da un malware o hacker(black).
- Attacchi mirati per l'ottenimento dei dati o credenziali dei clienti.

Interruzione dei servizi cloud

- Guasti hardware o errori umani che causano la sospensione dei servizi cloud, compromettendo la fiducia da parte dei clienti.
- Attacchi DDoS che opprime i sistemi interrompendo i servizi.

Danneggiamento della sicurezza e delle infrastrutture

- Mancato controllo di accessi che permetterebbero di consentire accessi non autorizzati a utenti sconosciuti.
- Vulnerabilità nella configurazione dell'infrastruttura cloud, un malintenzionato potrebbe sfruttare per accedere ai dati sensibili o per interrompere i servizi.

Attacchi informatici e malware

- Attacchi di tipo phishing mirati ai dipendenti dell'azienda per l'ottenimento di credenziali di accesso o implementazione di malware (trojan) nei sistemi.
- Divulgazione di malware attraverso software non aggiornati.

Perdita di reputazione e di fiducia da parte dei clienti

- Violazione dei dati che danneggiano la reputazione dell'azienda e minano la fiducia dei clienti.
- Servizi lenti o inefficaci agli incidenti di sicurezza che possono danneggiare la reputazione aziendale.

Possiamo dire che queste minacce rappresentano una gamma di rischi per gli asset critici dell'azienda e devono essere gestiti attraverso misure di sicurezza appropriate e una risposta tempestiva agli incidenti.

1.3 Analisi delle vulnerabilità

Le vulnerabilità: includono qualsiasi falla nel software utilizzato o nella configurazione di sicurezza dell'azienda che potrebbe essere sfruttata da attaccanti per accedere ai dati sensibili.

1.3.1 Identificazione delle vulnerabilità

Insufficiente protezione dell'accesso

Una cattiva gestione delle credenziali di accesso o delle politiche di autorizzazione può portare a accessi non autorizzati ai servizi cloud. Questo può avvenire attraverso falle nelle politiche di accesso, attacchi di phishing o sfruttando debolezze nei controlli di autenticazione.

Mancanza di isolamento dei dati

Se i dati dei diversi clienti sono archiviati o elaborati all'interno dello stesso ambiente cloud senza adeguato isolamento, potrebbe verificarsi un rischio di compromissione dei dati attraverso attacchi laterali o sfruttando vulnerabilità nel sistema di virtualizzazione.

Scarsa gestione degli aggiornamenti

La mancata applicazione di patch di sicurezza o la mancata gestione delle vulnerabilità note nei componenti software utilizzati per erogare i servizi cloud possono esporre il sistema a rischi di sicurezza. Gli attaccanti potrebbero sfruttare queste vulnerabilità per ottenere l'accesso non autorizzato o compromettere i dati.

Scarsa resilienza ai fallimenti

I servizi cloud dovrebbero essere progettati per essere resilienti ai fallimenti, ma una mancata progettazione o implementazione potrebbe portare a rischi di perdita di dati o interruzione del servizio in caso di guasti hardware o errori umani.

1.4 Analisi dell’impatto

L’impatto di una violazione dei dati può essere devastante. Oltre ai potenziali costi finanziari dovuti a sanzioni normative e risarcimenti ai clienti, l'azienda rischia di subire gravi danni reputazionali che potrebbero influenzare la fiducia dei clienti e la sua posizione sul mercato.

2. Analisi quantitativa del rischio

2.1 Determinazione della probabilità:

- La probabilità di una violazione dei dati è stimata al 70% (probabilità di incidente).
- L'azienda prevede che un incidente simile possa verificarsi in media due volte all'anno (**A**nnual **R**ate of **O**ccurrence**).**

  ARO = **n. Attacchi** / **anno**

2.2 Valutazione dell'impatto:

- Il costo stimato per una singola violazione dei dati è di 5 milioni di euro. (**S**ingle **L**oss **E**xpectancy)
- Questo include perdite finanziarie dovute a sanzioni normative, risarcimenti ai clienti e danni reputazionali.
- La perdita attesa (potenziale), su base annua, associata ad una specifica minaccia viene identificata come ALE (Annualized Loss Expectancy)

  ALE = SLE * ARO -> 5.000.000 € * 2 = 10.000.000 €

- Per calcolare la percentuale di impatto annua rispetto al fatturato annuale dell'azienda, utilizziamo l'Annual Loss Expectancy (ALE) che abbiamo calcolato in precedenza e il fatturato annuale dell'azienda

  I = percentuale di Impatto Annua = (ALE / Fatturato Annuale) * 100

  (10.000.000 € / 200.000.000) € * 100 = 5%

2.3 Calcolo del rischio:

- Rischio annuale = Probabilità * Impatto * Numero medio di incidenti.
- Rischio annuale = 0,70 * 5.000.000 € * 2 = 7.000.000 €.

2.4 Rischio relativo al fatturato:

- Rischio relativo al fatturato = Rischio annuale / Fatturato annuale * 100.
- Rischio relativo al fatturato = 7.000.000 € / 200.000.000 € * 100 = 3,5 %

Metrica	Valore
Probabilità (V)	70%
Impatto per Incidente (SLE)	5 milioni €
ARO (Annual Rate of Occurrence)	2
ALE (Annual Loss Expectancy)	10 milioni €
Percentuale di Impatto Annua	5%

3. Analisi qualitativa del rischio

3.1 Stima della verosimiglianza

La stima della verosimiglianza secondo il framework NIST (National Institute of Standards and Technology) fornisce una valutazione della probabilità che una minaccia sfrutti una vulnerabilità specifica in un sistema o nell'ambiente di un'organizzazione.

Per determinare la verosimiglianza, si prendono in considerazione diversi fattori, tra cui la presenza e la diffusione della minaccia, la complessità e l'efficacia delle contromisure, e il grado di esposizione della vulnerabilità. Basandoci sulle informazioni fornite:

- La minaccia di violazione dei dati sembra essere elevata, considerando l'importanza dei dati sensibili gestiti dall'azienda e la frequenza delle violazioni dei dati nell'ambiente cloud.
- Le contromisure di sicurezza possono essere implementate, ma la complessità del sistema cloud potrebbe rendere difficile la gestione di tutte le vulnerabilità.
- L'esposizione alla vulnerabilità potrebbe essere significativa, data la complessità del sistema cloud e il numero potenziale di punti di accesso.

Basandosi sulla stima che la probabilità di un incidente di questo tipo sia del 70%, secondo la seguente tabella il livello di verosimiglianza è "*Moderata*" - "*Se l'evento di minaccia viene avviato o si verifica, è probabile che abbia effetti negativi*".

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.

3.2 Stima dell'impatto

Basandosi sul calcolo effettuato al punto 2 del presente report l'impatto relativo alla perdita dei dati sul business dell'azienda è del 5%, secondo la seguente tabella il livello d'impatto è "*Basso*"- "*Si può prevedere che l'evento di minaccia abbia un effetto negativo limitato sulle operazioni organizzative, beni organizzativi, individui, altre organizzazioni o la Nazione. Un effetto negativo limitato significa che, ad esempio, l'evento di minaccia potrebbe: (i) causare un degrado della capacità della missione ad un misura e durata in cui l'organizzazione è in grado di svolgere le sue funzioni primarie, ma il l'efficacia delle funzioni è notevolmente ridotta; (ii) comportare lievi danni organizzativi risorse; (iii) comportare perdite finanziarie minori; o (iv) provocare danni minori alle persone.*"

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; (iii) 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.

3.3 Stima del rischio

Sfruttando le tabelle dei due punti precedenti, applicando i risultati alla tabella seguente, si può stimare il grado di rischio che come possiamo vedere è "*Basso*".

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

3.4 Descrizione del rischio

"*Rischio basso*" significa che ci si può aspettare che un evento minaccioso abbia un effetto negativo limitato operazioni organizzative, beni organizzativi, individui, altre organizzazioni o la Nazione.

TABLE I-3: ASSESSMENT SCALE – LEVEL OF RISK

Qualitative Values	**Semi-Quantitative Values**		**Description**
Very High	96-100	10	**Very high risk** means that a 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	**High risk** means that a threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Moderate	21-79	5	**Moderate risk** means that a threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Low	5-20	2	**Low risk** means that a threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Very Low	0-4	0	**Very low risk** means that a threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.