Report: Analisi del rischio

26/04/2024

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.

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

Introduzione

In questo contesto, un'azienda di servizi cloud si trova esposta al rischio di violazione dei dati a causa di vulnerabilità nel software e nelle configurazioni di sicurezza. La probabilità di un incidente di questo tipo è stata stimata al 70%, con potenziali impatti finanziari significativi dovuti a sanzioni normative, risarcimenti ai clienti e danni reputazionali.

Al fine di valutare e gestire in modo efficace questo rischio, è stata condotta un'analisi approfondita utilizzando un approccio semi-quantitativo basato sulle migliori pratiche e sulle linee guida della normativa NIST SP800-30R. Questo report presenta i risultati di tale analisi, fornendo raccomandazioni per migliorare la sicurezza dei dati e mitigare il rischio di violazioni future.

Contesto

Si ipotizza che l'azienda operi principalmente in diversi paesi europei, inclusa l'Italia. Per quanto riguarda le sanzioni normative in Italia, possiamo considerare la Legge Europea sulla Protezione dei Dati Personali (GDPR) che prevede multe fino al 4% del fatturato annuo globale dell'azienda o fino a 20 milioni di euro, a seconda di quale sia il valore maggiore.

1. Sanzioni Normative = 0,04 x 200.000.000 = 8.000.000 euro

Viene considerata quindi una multa di 20.000.000 di euro (è il valore maggiore).

I costi di risarcimento per i clienti potrebbero variare a seconda del tipo di dati violati e del numero di clienti coinvolti. Ad esempio, stimiamo un costo medio per cliente danneggiato di 500 euro. Considerando 200.000 clienti totali e solo ¼ di essi sono stati violati. A questo valore va aggiunto il costo medio del tempo e le risorse necessarie per informare, assistere e risarcire ogni cliente colpito da una violazione dei dati di 100 euro per cliente.

Costi Clienti = 500 + 100 (Spese tempo, informare, assistere) = 2300 euro/cliente

2. Costi totali dei clienti = 600 x 200.000/4 = 30.000.000 euro

Per quanto riguarda i danni reputazionali, possiamo fare una stima in base al fatturato dell'azienda. Supponiamo che una violazione dei dati possa causare un calo del 5% delle entrate annue dell'azienda, considerando la perdita di fiducia dei clienti e l'effetto negativo sulla percezione del marchio.

3. Costi Reputazionali = 0,05 x 200.000.000 = 10.000.000 euro

Tabella Dati

Parametro	Value
V(verosomiglianza)	70%
SLE (Single Loss Expectancy)	5.000.000 euro
ARO (Annualized Rate of Occurrence)	2 attacchi/anno
Sanzioni Normative	20.000.000 euro
Costo totale dei clienti	30.000.000 euro
Costi Reputazionali	10.000.000

La tabella dei dati fornisce una panoramica dei parametri utilizzati per l'analisi del rischio, inclusi i valori di verosimiglianza, la singola perdita attesa, la frequenza annuale degli attacchi e i costi associati alle sanzioni normative, ai risarcimenti dei clienti e ai danni reputazionali.

Analisi semi-quantitativa del rischio

L'analisi del rischio semi-quantitativa è un metodo per valutare i rischi che combina elementi qualitativi e quantitativi. Solitamente si parte da rilevazioni che permettono di definire valori oggettivi di verosomiglianza, impatto e rischio (analisi quantitativa) per poi utilizzare metodi dell'analisi qualitativa per ottenere una relazione con standard e/o regolamentazioni. Alternativamente, si possono definire valori numerici di verosomiglianza, impatto e rischio in modo soggettivo, avvicinandosi maggiormente all'analisi qualitativa così da sfruttare metodi matematici per poter effettuare operazioni tra valori (es. valore min/max, media, moltiplicazione, differenza) e trarre conclusioni o relazionarsi sempre con standard e/o regolamentazioni.

Definizione del valore % dell'impatto

Per calcolare il valore di impatto totale di questo rischio, possiamo utilizzare la formula dell'Annualized Loss Expectancy (ALE), che tiene conto sia della probabilità di un incidente in un anno (Annual Rate of Occurrence - ARO) che del costo stimato di ciascun incidente singolo (Single Loss Expectancy – SLE). L'SLE comprende il costo stimato di una singola violazione dati (5.000.000) a cui vengono sommati i costi delle sanzioni normative, costo totale dei clienti ed i costi reputazionali.

- SLE = 5.000.000 + 30.000.000 + 10.000.000 + 20.000.000 = 65.000.000 euro/attacco

L'ALE viene calcolato con la seguente formula:

- ALE = SLE x ARO
- ALE = 65.000.000 x 2 = 130.000.000 euro/anno

Con il valore di ALE è possibile calcolare il valore di impatto totale percentuale.

- I = ALE/fatturato annuo x 100 = 130.000.000/200.000.000 x 100 = 65%

L'analisi semi-quantitativa del rischio adottata integra elementi qualitativi e quantitativi per fornire una valutazione completa dei rischi. Questo approccio permette di ottenere una stima accurata del valore di impatto complessivo, considerando sia gli aspetti finanziari che quelli non finanziari.

Definendo il valore percentuale di impatto, possiamo calcolare il valore di impatto totale in percentuale rispetto al fatturato annuo dell'azienda. In questo caso specifico, il valore di impatto è del 65%, indicando il peso significativo che questo rischio potrebbe avere sulle attività aziendali.

Analisi qualitativa

Dopo aver ottenuto il valore di impatto totale percentuale attraverso l'analisi semi-quantitativa del rischio, è importante integrare questa valutazione con un'analisi qualitativa approfondita utilizzando le tabelle della normativa NIST SP800-30R.

Questa analisi consentirà di esaminare più nel dettaglio la probabilità che l'impatto si trasformi in un evento avverso, valutare l'impatto del threat event e determinare il livello complessivo di rischio.

Correlazione dei dati con le Tabelle NIST SP800-30r

Le tabelle di riferimento utilizzate per questa correlazione di dati sono: G-4, H-3 e I-2.

La Tabella G-4 della normativa NIST SP800-30R, intitolata "Assessment Scale - Likelihood of Threat Event Resulting in Adverse Impacts", fornisce una scala di valutazione per determinare la probabilità che un evento minaccioso possa provocare impatti negativi sull'organizzazione. Questa scala aiuta a quantificare la verosimiglianza di un evento minaccioso che si traduce in conseguenze avverse. Considereremo quindi, il valore di verosomoglianza dell'evento in esame:

- V = 70%

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.

L'evento in esame rientra nella fascia " Moderato ", il che indica in modo molto probabile che abbia un impatto negativo.

La Tabella H-3 della normativa NIST SP800-30R, denominata "Assessment Scale - Impact of Threat Events", fornisce una scala di valutazione per determinare l'impatto degli eventi minacciosi sull'organizzazione. Questa scala aiuta a valutare la gravità delle conseguenze di un evento minaccioso, consentendo agli analisti del rischio di comprendere appieno l'entità degli impatti che potrebbero verificarsi. Per la valutazione di questa tabella considereremo il valore dell'Impatto per questo evento:

- I = 65%

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.

L'evento rientra nella fascia " Moderato ". L'evento minaccioso potrebbe essere previsto di avere un grave effetto negativo sulle operazioni dell'organizzazione, sugli asset organizzativi, sulle persone, su altre organizzazioni o sulla Nazione. Un grave effetto negativo significa che, ad esempio, l'evento minaccioso potrebbe: (i) causare una significativa degradazione della capacità operativa a un livello e per una durata tale da consentire all'organizzazione di svolgere le sue funzioni principali, ma con un significativo ridimensionamento dell'efficacia delle funzioni stesse; (ii) provocare danni significativi agli asset organizzativi; (iii) provocare una perdita finanziaria significativa; o (iv) causare un danno significativo alle persone che non comporta la perdita della vita o gravi lesioni minaccianti la vita.

La Tabella I-2 della normativa NIST SP800-30R, denominata "Assessment Scale - Level of Risk (Combination of Likelihood and Impact)", fornisce una scala di valutazione per determinare il livello

complessivo di rischio associato a un particolare evento minaccioso. Questa scala combina la probabilità dell'evento minaccioso di verificarsi (likelihodd) con l'impatto che l'evento potrebbe avere sull'organizzazione (impact), offrendo una visione integrata della gravità del rischio.

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

La correlazione dei dati ottenuti consultando la tabella della probabilità che l'evento si verifichi con la tabella dell'impatto è di livello " Moderato ".

Il rischio moderato implica che ci si potrebbe aspettare che un evento minaccioso abbia un grave effetto negativo sulle operazioni dell'organizzazione, sugli asset organizzativi, sulle persone, su altre organizzazioni o sulla Nazione.

Raccomandazioni

Implementare Misure di Sicurezza Aggiuntive: Considerando la probabilità moderata di una violazione dei dati e il suo potenziale impatto significativo, si consiglia di implementare misure di sicurezza aggiuntive per rafforzare la protezione dei sistemi e dei dati dell'azienda. Ciò potrebbe includere l'adozione di tecnologie di sicurezza avanzate, come la crittografia dei dati e l'autenticazione multi-fattore, e l'implementazione di politiche di sicurezza rigorose.

Migliorare la Consapevolezza sulla Sicurezza: Investire nella formazione e nella sensibilizzazione del personale riguardo alle pratiche di sicurezza informatica è fondamentale per ridurre il rischio di violazioni dei dati. Creare programmi di formazione regolari e fornire risorse educative sulle best practice di sicurezza può aiutare a garantire che tutto il personale sia consapevole delle minacce e delle misure preventive da adottare.

Pianificare e Testare la Risposta agli Incidenti: Prepararsi per il peggio è essenziale in caso di violazione dei dati. Si consiglia di sviluppare e testare un piano di risposta agli incidenti dettagliato, che delinei le procedure da seguire in caso di violazione e assegni chiaramente le responsabilità. Condurre regolarmente esercitazioni di simulazione degli incidenti può contribuire a garantire che il personale sia pronto a gestire efficacemente eventuali emergenze.

Monitorare e Aggiornare Costantemente le Misure di Sicurezza: Il panorama delle minacce informatiche è in continua evoluzione, pertanto è importante monitorare costantemente l'ambiente IT e aggiornare regolarmente le misure di sicurezza per affrontare le nuove minacce. Implementare un sistema di monitoraggio continuo della sicurezza e mantenere aggiornati i software e le patch di sicurezza può contribuire a ridurre il rischio di violazioni dei dati.

Conclusioni

In conclusione, l'analisi del rischio condotta mediante un approccio semi-quantitativo ha fornito una visione dettagliata e articolata dei potenziali impatti finanziari e reputazionali di una violazione dei dati all'interno dell'azienda di servizi cloud. I dati raccolti e analizzati, insieme alle valutazioni qualitative delle tabelle della normativa NIST SP800-30R, hanno consentito di identificare la probabilità che l'evento minaccioso si verifichi, nonché l'impatto potenziale che potrebbe avere sull'organizzazione.

L'analisi ha evidenziato che vi è una probabilità moderata che un incidente di violazione dei dati possa verificarsi, con un impatto significativo sulle operazioni aziendali, sugli asset, sui clienti, e sulla reputazione dell'azienda. In particolare, si prevede che l'evento minaccioso potrebbe causare gravi danni finanziari e danneggiare la fiducia dei clienti nel marchio dell'azienda.

L'utilizzo delle tabelle della normativa NIST SP800-30R ha contribuito a definire il livello di rischio complessivo associato alla violazione dei dati, consentendo agli analisti del rischio di valutare in modo accurato la probabilità e l'impatto degli eventi minacciosi e di identificare le aree critiche che richiedono un'attenzione prioritaria.

In definitiva, questa analisi del rischio fornisce una base solida per lo sviluppo di strategie di mitigazione del rischio mirate ed efficaci, che possono contribuire a proteggere l'azienda da potenziali perdite finanziarie e danni reputazionali derivanti da violazioni dei dati.