Calcolo del Fattore di Rischio: Guida Completa

Introduzione

Il calcolo del fattore di rischio rappresenta un elemento cruciale nella gestione della sicurezza informatica, specialmente per piattaforme e-commerce. Comprendere i rischi permette di sapere quali asset, minacce e vulnerabilità hanno il maggiore impatto sull' organizzazione, supportando decisioni strategiche per la protezione dei dati e la conformità normativa.

Questa guida accompagna il lettore passo passo nella valutazione del rischio, integrando spiegazioni dettagliate, formule di calcolo, esempi pratici e riferimenti agli standard internazionali come NIST, OWASP, PCI DSS e GDPR.

Componenti della Valutazione del Rischio

Il rischio nasce dall' interazione tra la probabilità che un evento si verifichi e l' impatto che questo evento può avere sugli asset dell' azienda.

Gli Asset

Gli asset sono le risorse critiche dell' organizzazione: possono essere piattaforme web, database clienti, sistemi di pagamento, infrastruttura IT o dati sensibili come le informazioni delle carte di credito.

Ogni asset viene valutato considerando il valore aziendale, ovvero quanto esso è strategico, e la sensibilità dei dati che contiene. Entrambe le dimensioni vengono misurate su una scala da 1 a 5, dove 5 indica massima rilevanza o massima riservatezza.

Le Minacce

Le minacce rappresentano eventi che possono arrecare danno agli asset. Possono essere attacchi informatici come SQL Injection, XSS, DDoS o phishing, ma anche errori umani, guasti dei sistemi o minacce interne.

Ogni minaccia viene valutata in termini di frequenza, che indica quanto è probabile il suo verificarsi, e di sofisticazione, che rappresenta il livello di complessità dell'attacco. Entrambi i valori sono misurati su una scala da 1 a 5.

Le Vulnerabilità

Le vulnerabilità sono debolezze all'interno degli asset che possono essere sfruttate dalle minacce. Possono riguardare controlli di accesso insufficienti, errori di configurazione, componenti software non aggiornati o fallimenti crittografici.

Ogni vulnerabilità viene valutata secondo sfruttabilità (facilità con cui può essere sfruttata) e difficoltà di rilevamento (quanto è complesso identificarla), entrambe su scala 1–5.

Il Calcolo del Fattore di Rischio

Il fattore di rischio deriva dalla combinazione di probabilità e impatto. La probabilità indica quanto è probabile che una minaccia sfrutti una vulnerabilità, mentre l'impatto misura le conseguenze sul business e sulla sicurezza dei dati.

Probabilità

La probabilità può essere stimata con la formula:

$$\text{Probabilità} = \frac{\text{Frequenza della minaccia} + \text{Sfruttabilità della vulnerabilità}}{2}$$

Questo valore viene normalizzato su una scala da 1 a 5.

Impatto

L'impatto valuta le conseguenze della minaccia sull'asset e tiene conto del valore aziendale e della sensibilità dei dati, adattato dalla sofisticazione della minaccia:

$$\text{Impatto} = \frac{\text{Valore Aziendale} + \text{Sensibilità Dati}}{2} \times \text{Moltiplicatore Minaccia}$$

dove il moltiplicatore dipende dalla sofisticazione della minaccia:

$$\text{Moltiplicatore Minaccia} = 1 + 0.2 \times (\text{Sofisticazione} - 1)$$

L'impatto finale viene anch'esso normalizzato su una scala da 1 a 5.

Punteggio di Rischio

Il punteggio di rischio combina probabilità e impatto:

$$\text{Rischio} = \text{Probabilità} \times \text{Impatto}$$

Il risultato permette di definire il livello di rischio, dalla valutazione molto bassa fino a quella critica.

Esempio Pratico

Consideriamo un database clienti con valore aziendale pari a 4 e sensibilità dei dati pari a 5. Una minaccia di tipo SQL Injection ha frequenza 4 e sofisticazione 3, mentre la vulnerabilità Injection ha sfruttabilità 4 e difficoltà di rilevamento 3.

Calcolando la probabilità:

$$\text{Probabilità} = \frac{4 + 4}{2} = 4$$

Calcolando l'impatto:

$$\text{Impatto base} = \frac{4 + 5}{2} = 4.5$$

$$\text{Moltiplicatore minaccia} = 1 + 0.2 \times (3 - 1) = 1.4$$

$$\text{Impatto finale} = 4.5 \times 1.4 = 6.3 \quad (\text{normalizzato a } 5)$$

Punteggio di rischio:

$$\text{Rischio} = 4 \times 5 = 20 \quad \Rightarrow \text{Livello Alto}$$

Mitigazione e Conformità

Per ogni rischio identificato è possibile definire azioni correttive, come aggiornamenti software, controlli accessi, crittografia, firewall o monitoraggio continuo.

In parallelo, è importante considerare l’ impatto sulla conformità: * PCI DSS: tutela dei dati delle carte di credito * GDPR: sicurezza dei dati personali (Art. 32) * Misure Minime AgID: requisiti ICT per le pubbliche amministrazioni

Applicazioni del Documento

Questa guida non si limita alla teoria: offre strumenti concreti per PMI che vogliono avviare un processo strutturato di valutazione del rischio, supporta Security Officer e DPO nelle decisioni strategiche, e costituisce un caso di studio pratico per consulenti, auditor e corsi di formazione in cybersecurity.