Documento Esplicativo sul Calcolo del Fattore di Rischio

Introduzione

Nel mondo dell'e-commerce, la sicurezza informatica non è solo una necessità tecnica, ma un elemento strategico che può influenzare direttamente la reputazione, la fiducia dei clienti e la continuità operativa di un'azienda. Per un e-commerce di abbigliamento, le principali aree di interesse includono la protezione dei dati personali dei clienti, la sicurezza delle transazioni finanziarie e l'integrità dei sistemi digitali.

Questo documento offre una guida completa al calcolo del fattore di rischio, integrando metodologie riconosciute come il NIST Cybersecurity Framework, le linee guida OWASP, gli standard PCI DSS e le disposizioni del GDPR. L'obiettivo è fornire uno strumento utile sia agli specialisti di sicurezza sia agli stakeholder aziendali.

Il Concetto di Rischio

Il rischio in ambito informatico rappresenta la combinazione della probabilità che un evento dannoso si verifichi e dell'impatto che tale evento avrebbe sugli asset aziendali. Gli asset includono risorse fondamentali come il sito web, il database dei clienti, i sistemi di pagamento, i server e l'infrastruttura IT in generale.

Le minacce sono eventi potenzialmente dannosi, mentre le vulnerabilità rappresentano le debolezze che le minacce possono sfruttare. Analizzando come questi elementi interagiscono, è possibile identificare scenari di rischio specifici e prioritizzare le azioni di mitigazione.

Gli Asset

Gli asset aziendali principali in un e-commerce di abbigliamento includono:

- Sito web: piattaforma di vendita online, fondamentale per disponibilità e sicurezza dei dati.
- Database clienti: contiene informazioni sensibili, inclusi dati personali e preferenze.
- Sistema di pagamento: gestisce transazioni finanziarie e deve rispettare standard di sicurezza elevati.
- Infrastruttura IT: server, reti e applicazioni di supporto.

Per ogni asset si valuta il valore business e la sensibilità dei dati, per stimare il rischio associato.

Minacce e Vulnerabilità

Le minacce possono essere attacchi informatici, errori umani, guasti dei sistemi o eventi naturali. Esempi tipici includono SQL Injection, Cross-Site Scripting (XSS), Phishing o guasti hardware.

Le vulnerabilità sono debolezze dei sistemi che le minacce possono sfruttare, come controlli di accesso insufficienti, fallimenti crittografici o componenti software vulnerabili. La combinazione di minaccia e vulnerabilità determina uno scenario di rischio.

Calcolo del Fattore di Rischio

Il fattore di rischio è calcolato considerando:

- Probabilità: quanto è probabile che una minaccia sfrutti una vulnerabilità.
- Impatto: gravità delle conseguenze sull'asset.

La probabilità tiene conto della frequenza della minaccia e della facilità di sfruttamento della vulnerabilità. L'impatto considera il valore dell'asset e la sensibilità dei dati, modulati dalla sofisticazione della minaccia. La

moltiplicazione di probabilità e impatto produce un punteggio numerico, classificato in livelli qualitativi da "molto basso" a "critico".

Questo approccio aiuta a identificare e prioritizzare gli scenari di rischio più rilevanti.

Misure di Mitigazione

Per ogni vulnerabilità sono suggerite azioni concrete:

- Controlli di accesso più rigorosi.
- Crittografia robusta per dati in transito e a riposo.
- Validazione completa di input e query per prevenire injection.
- Monitoraggio continuo delle attività sospette tramite SIEM.

Gli scenari di rischio vengono inoltre valutati rispetto alla conformità normativa, come GDPR per dati personali e PCI DSS per dati delle carte di credito, oltre alle misure minime ICT AgID.

Esempi Pratici

Un attacco SQL Injection sul database clienti ad alto rischio richiede query parametrizzate, validazione dell'input, controlli di accesso rafforzati e monitoraggio continuo. L'impatto normativo richiede interventi immediati per conformità GDPR e PCI DSS.

Un errore umano nella configurazione di un server può avere un impatto critico nonostante una probabilità moderata, evidenziando la necessità di audit regolari e procedure operative standardizzate.

Monitoraggio e Miglioramento Continuo

La valutazione del rischio deve essere aggiornata regolarmente. L'integrazione con sistemi di monitoraggio e gestione eventi di sicurezza consente di raccogliere dati reali e aggiornare dinamicamente la valutazione. Coinvolgere più esperti riduce la soggettività delle stime.