INCIDENT RESPONSE

W20D4 - Pratica

Azioni Preventive:

Per ridurre il rischio di un attacco SQL Injection e XSS Cross-Site Scripting è possibile intraprendere le seguenti migliorie:

Approccio Zero-Trust: Con questo metodo di sicurezza è necessario dimostrare di essere effettivamente l'utente che si necessita e verranno forniti solo i privilegi necessari.

Implementazione di query parametrizzate che possono proteggere dagli attacchi.

Controllo Firewall: Implementare una whitelist per gli utenti da autorizzare, utilizzare un Web Application Firewall (WAF) essi devono essere aggiornati per rispondere alle nuove minacce ed evitare che vengano sfruttate vulnerabilità presenti nelle versioni obsolete.

Aggiunta di flag all'interno del sito come HttpOnly, SameSite e Secure.

Impatti su Business:

L'attacco DDoS subito precedentemente ha avuto una durata complessiva di circa 10 minuti e causando una perdita di circa 15000€, per ovviare al problema e fare in modo che non si ripeta è possibile adottare soluzioni che mitigano gli attacchi DDoS-Guard, Cloudflare DDoS Protection o simili valutandoli e scegliendoli in base alle esigenze, se l'attacco venisse ripetuto con frequenza potrebbe essere necessario adottare ulteriori misure al fine di mantenere il sito operativo quali; Migliorare l'infrastruttura di hosting, suddividere il carico su più data center, richiedere una verifica anti bot all'accesso del sito nel caso venisse attaccato ed inserire una blacklist temporanea degli IP e User-agent che vengono utilizzati per l'attacco.

Soluzione definitiva:

Come soluzione definitiva in linea generale possiamo adottare la separazione dell'ambiente compromesso in modo da conservare il malware e rendere comunque il servizio accessibile tramite un ripristino. Possono essere utili anche controlli sui privilegi quando si accede da internet al sito di e-commerce e di impostare controlli più stringenti sui firewall e le policy di accesso.