Incident response (Modulo 5, Master Cybersecurity)

Azioni Preventive:

1. Utilizzare query parametrizzate per l'interazione con il database. Questo impedisce agli attaccanti di iniettare codice SQL malevolo nelle tue query.
2. Eseguire una rigorosa validazione e filtraggio degli input dell'utente, assicurandosi che siano conformi alle aspettative. Ad esempio, verificare che gli input numerici siano effettivamente numeri. Si può utilizzare anche per evitare attacchi XSS.
3. Concedere solo privilegi minimi necessari al database per eseguire le operazioni richieste.
4. Assicurarsi che il tuo team di sviluppo sia ben formato sulla sicurezza delle applicazioni web e segua le migliori pratiche di sviluppo sicuro.

Impatto sul business:

Impatto economico = Guadagno medio al minuto x Tempo di indisponibilità x Numero di utenti
Impatto economico = 1500€/minuto x 10 minuti x utenti

Azioni preventive:

1. Progettare l'infrastruttura in modo che possa rispondere a picchi di traffico, distribuendo il carico su più server o istanze in modo da resistere meglio agli attacchi DDoS.
2. Configura regole di firewall e filtri di rete per limitare il traffico proveniente da indirizzi IP sospetti o noti per essere coinvolti in attacchi DDoS.
3. Implementare sistemi di monitoraggio avanzati per identificare attacchi DDoS in corso in modo proattivo e prendere misure rapide per mitigarli.

Response:

La prima cosa da fare è isolare la macchina infettata dalla rete. Questo può essere fatto bloccando o limitando le connessioni in uscita della macchina tramite il firewall o altri mezzi. In questo modo, si impedisce al malware di comunicare con altri dispositivi sulla rete.

Una volta isolata la macchina infettata, è possibile eseguire un'analisi approfondita del malware per comprenderne il funzionamento, le vulnerabilità che potrebbero essere sfruttate e le azioni che compie.

Identificare e rimuovere il malware dalla macchina infettata. Questo può richiedere l'utilizzo di strumenti di scansione antivirus/antimalware o l'intervento manuale di esperti di sicurezza informatica.

Nel caso specifico, bisognerà “sganciare” il FLUSSO APPLICAZIONE – RETE INTERNA (freccia azzurra), in modo che l’attaccante non possa arrivare alla rete interna.