W20D4

Azioni preventive: quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni

1.Per difendere una Web Application da attacchi di tipo XSS e SQLi si potrebbe sicuramente aggiungere un Web Application Firewall posizionato tra il firewall principale e la DMZ , bloccando richieste malevole e attacchi come SQLi e XSS.
Un altro metodo potrebbe essere assicurarsi che le credenziali del database abbiano il minimo privilegio necessario o anche implementare una Content Security Policy per limitare le fonti da cui il browser può caricare contenuti.

Impatti sul business: l'applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione non raggiungibile per 10 minuti. Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media ogni minuto gli utenti spendono 1.500 € sulla piattaforma di e-commerce. Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica

L'applicazione e-commerce subisce un attacco DDoS che la rende irraggiungibile per 10 minuti. Dato che ogni minuto gli utenti spendono in media 1.500 €, l'impatto economico è calcolabile come segue:

- Tempo di inattività: 10 minuti
- Perdita per minuto: 1.500 €
- Perdita totale: 1.500 € * 10 = 15.000 €

Per prevenire gli attacchi di tipo DDoS abbiamo diversi metodi come ad esempio:

- Mitigazione DDoS: un servizio di mitigazione DDoS (es. Cloudflare) filtra il traffico anomalo prima che raggiunga il firewall.
- monitorare costantemente il traffico di rete e impostare degli alert per attività sospette o picchi di traffico anomali
- Avere sempre un backup in caso di disastro

Response: l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata.

Se la Web Application viene infettata da un malware ,la priorità è la segmentazione della rete: la rete interna è suddivisa in sottoreti isolate per limitare i movimenti laterali del malware.Isolamento del server compromesso: il firewall blocca immediatamente qualsiasi comunicazione tra la DMZ e la rete interna, mantenendo il server infetto isolato,indicare un sistema di backup per garantire che i dati non vengano compromessi in caso di ulteriore propagazione,utilizzare un Web Application Firewall per impedire il traffico non autorizzato