Traccia:

Con riferimento alla figura in slide 2, rispondere ai seguenti quesiti.

1. 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

2. 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

3. 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. Modificate la figura in slide 2 con la soluzione proposta.

4. Soluzione completa: unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)

5. Modifica più aggressiva dell'infrastruttura (se necessario/facoltativo magari integrando la soluzione al punto 2)

1. Per difendere l'applicazione di e-commerce da attacchi di tipo SQLi e XSS all'interno di una rete con una DMZ (Zona Demilitarizzata), è necessario implementare le seguenti azioni preventive:

    - Segmentazione della rete: Assicurarsi che la rete interna e la DMZ siano adeguatamente segmentate tramite firewall e politiche di rete per limitare l'accesso non autorizzato dalla DMZ alla rete interna.
    - Implementazione di un WAF: Installare un Web Application Firewall (WAF) nella DMZ per filtrare e monitorare il traffico HTTP/HTTPS in arrivo per rilevare e bloccare attacchi XSS e SQLi.
    - Validazione dei dati in input: Verificare e sanitizzare rigorosamente tutti i dati in input ricevuti dall'utente prima di elaborarli o inserirli in query SQL per prevenire attacchi SQLi.
    - Codifica dei dati di output: Assicurarsi che tutti i dati restituiti agli utenti siano correttamente codificati per prevenire attacchi XSS.

    Modificando la figura per evidenziare le implementazioni, si potrebbe aggiungere un blocco rappresentante il WAF posizionato tra la DMZ e Internet, con frecce che indicano il flusso del traffico attraverso il WAF per essere filtrato e monitorato. Inoltre, si potrebbero aggiungere etichette o descrizioni per indicare i punti di validazione dei dati in input, l'utilizzo di parametri preparati e altre misure di sicurezza implementate nella rete.

2. Per calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio per 10 minuti, possiamo utilizzare la seguente formula:

    Impatto sul business = (Durata dell'interruzione) * (Perdita di guadagno al minuto)

Dove:

- Durata dell'interruzione è 10 minuti.
- Perdita di guadagno al minuto è 1.500 €.

Quindi:

Impatto sul business = 10 minuti * 1.500 €/minuto = 15.000 €

Quindi, l'impatto sull'attività dovuto a 10 minuti di interruzione del servizio è di 15.000 €.

Per quanto riguarda le azioni preventive, ci sono diversi approcci che si possono adottare per mitigare gli attacchi DDoS e ridurre l'impatto sul business:

- Implementazione di un sistema di mitigazione DDoS**: Utilizzare servizi o dispositivi specializzati che possono rilevare e mitigare gli attacchi DDoS in tempo reale.
- Bilanciamento del carico: Distribuire il carico del traffico su più server può aiutare a ridurre l'impatto degli attacchi DDoS.

- Firewall e filtri IP: Configurare firewall e filtri IP per bloccare o limitare l'accesso ai clienti sospetti o provenienti da fonti non attendibili.

- Monitoraggio continuo del traffico di rete: Utilizzare strumenti di monitoraggio del traffico di rete per rilevare anomalie e comportamenti sospetti che potrebbero essere indicativi di un attacco DDoS in corso.

- Pianificazione di capacità: Avere risorse aggiuntive disponibili per gestire picchi di traffico improvvisi può aiutare a mantenere il servizio operativo anche durante gli attacchi DDoS.

- Backup e ripristino dei dati: Assicurarsi di avere procedure di backup e ripristino dei dati in caso di perdita di dati a causa di un attacco DDoS o di altri eventi catastrofici.

- Pianificazione della risposta agli incidenti: Avere un piano di risposta agli incidenti ben definito può aiutare a mitigare gli effetti degli attacchi DDoS e ripristinare rapidamente il servizio.

3. Per proteggere la rete interna dall'infezione da malware sull'applicazione Web, senza rimuovere l'accesso all'attaccante alla macchina infettata, possiamo implementare diverse azioni preventive. Inoltre, è importante mantenere l'accessibilità dell'applicazione e-commerce per gli utenti tramite Internet. Ecco alcune azioni che potremmo adottare:

    - Segmentazione della rete: Isolare il server compromesso in una zona separata della rete, come una subnet dedicata, per limitare la propagazione del malware verso altri dispositivi nella rete interna.

- Implementazione di controlli di sicurezza avanzati: Utilizzare soluzioni di sicurezza avanzate come sistemi di rilevamento delle intrusioni (IDS) e sistemi di prevenzione delle intrusioni (IPS) per identificare e bloccare il traffico dannoso prima che possa raggiungere altri dispositivi nella rete interna.

- Monitoraggio del traffico di rete: Monitorare costantemente il traffico di rete per individuare eventuali attività sospette o tentativi di propagazione del malware e intervenire tempestivamente.

- Politiche di accesso restrittive: Configurare politiche di accesso rigorose per limitare l'accesso del server compromesso ad altre risorse nella rete interna, consentendo solo le connessioni necessarie per scopi di gestione e monitoraggio.

- Aggiornamenti regolari e patching: Assicurarsi che tutti i sistemi e le applicazioni siano aggiornati con le ultime patch di sicurezza per ridurre le vulnerabilità che potrebbero essere sfruttate dall'attaccante per compromettere altri dispositivi nella rete interna.

- Backup e ripristino dei dati: Mantenere regolarmente backup completi e aggiornati dei dati critici dell'applicazione e-commerce in modo che, in caso di infezione da malware, sia possibile ripristinare rapidamente i dati senza compromettere l'integrità della rete interna.

Per evidenziare queste implementazioni nella figura dell'architettura di rete, potremmo aggiungere etichette o colori distintivi per rappresentare le zone della rete, come la DMZ e la rete interna, e mostrare i flussi di traffico controllati attraverso dispositivi di sicurezza come firewall, IDS/IPS, e sistemi di monitoraggio del traffico. Inoltre, potremmo evidenziare il server compromesso e le misure adottate per isolare e controllare il suo accesso alla rete interna.