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**

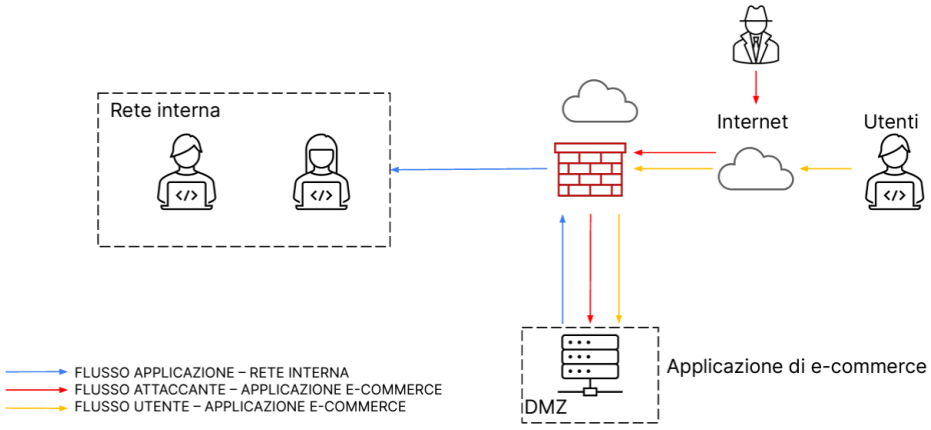
3. **Response**: l'applicazione Web viene infettata da un malware.
   La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata.
   Modificate la figura in slide 2 con la soluzione proposta.

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)**

Architettura di rete:
L'applicazione di e-commerce deve essere disponibile per gli utenti tramite Internet per effettuare acquisti sulla piattaforma.

La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.



AZIONI PREVENTIVE:

Considerata l'architettura di rete in questione, come primo step si dovrebbe procedere alla configurazione della DMZ e del Firewall come di seguito:

- **Regole del Firewall**:
  Configurare il firewall per limitare il traffico ai server della DMZ solo alle porte e ai servizi necessari.
  Bloccare tutto il traffico non necessario e monitorare i log del firewall per attività sospette.

- **Isolamento dei Servizi**:

Isolare i servizi critici nella DMZ e garantire che l'accesso alla rete interna avvenga solo attraverso canali strettamente controllati e autorizzati.

Per proteggere l'applicazione web da attacchi SQL Injection (SQLi) e Cross-Site Scripting (XSS) invece, è necessario adottare una serie di misure preventive a livello di sviluppo dell'applicazione, configurazione del server e sicurezza di rete.
Come primo passo:

Parametrizzazione delle Query:

- Utilizzare query parametrizzate per interagire con il database. Questo separa il codice SQL dai dati forniti dagli utenti, impedendo l'inserimento di codice potenzialmente dannoso. Si potrebbe utilizzare anche l'Object-Relational Mapping (ORM) o query builders che gestiscono automaticamente la parametrizzazione delle query, riducendo nettamente il rischio di SQLi.

Validazione e Sanitizzazione dei Dati:

- Validare e sanitizzare tutti i dati di input dell'utente lato server. Assicurarsi che i dati siano del tipo e del formato previsto impostando dei filtri di input nel codice della web app.

Web Application Firewall (WAF):

- Implementare un WAF per monitorare e filtrare traffico malevolo configurando regole specifiche per rilevare e bloccare tentativi di SQLi.

Evasione di Output (Output Encoding):

- Effettuare l'escaping dell'output quando si inseriscono dati non attendibili nelle pagine HTML. Trasformando i caratteri speciali che potrebbero essere interpretati come codice eseguibile dal browser in un formato sicuro, si possono evitare attacchi di tipo XSS.

  Quando si inseriscono dati non attendibili (come input dell'utente) in una pagina web, è essenziale eseguire l'output encoding per garantire che questi dati non vengano interpretati come codice HTML o JavaScript. L'output encoding è fondamentale per prevenire attacchi XSS, dove un aggressore tenta di iniettare codice maligno in pagine web visualizzate da altri utenti.

  Se i dati non vengono correttamente codificati, possono essere interpretati come script dal browser, permettendo all'aggressore di eseguire azioni

arbitrarie, come rubare cookie, manipolare contenuti della pagina, o eseguire altre azioni dannose.

IMPATTI SUL BUSINESS:

Prendendo in analisi questa possibilità, cioè che l'applicazione Web subisca un attacco di tipo DDoS dall'esterno che rende l'applicazione non raggiungibile per 10 minuti, calcolo l'impatto sul business, considerando che in media ogni minuto gli utenti spendono 1.500 € sulla piattaforma di e-commerce.

Se ogni minuto gli utenti spendono in media 1.500 € sulla piattaforma di e-commerce, l'impatto economico di 10 minuti di inattività può essere calcolato come segue:

Impatto Economico = Perdita per Minuto × Durata dell'Interruzione

Dove:

Perdita per Minuto = ***1.500 €***
Durata dell'Interruzione = ***10 minuti***

Quindi:

Impatto Economico = 1.500 € × 10 = ***15.000 €***

Un attacco DDoS (Distributed Denial of Service) può avere impatti significativi su un'azienda, specialmente su una piattaforma di e-commerce. In questo scenario, l'impatto economico per soli 10 minuti di inattività, sarebbe di 15.000 €.

Risulta, perciò, importante e necessario, implementare misure preventive per proteggere l'applicazione web da futuri attacchi DDoS, ad esempio:

- **Content Delivery Network (CDN)**:
  Utilizzare una CDN come Cloudflare, Akamai o Amazon CloudFront può aiutare a distribuire il traffico e assorbire gli attacchi DDoS. Le CDN dispongono di infrastrutture globali che possono gestire grandi volumi di traffico e filtrare quello dannoso.

- **Servizi di Protezione DDoS**:

Affidarsi a servizi di protezione DDoS come Cloudflare, AWS Shield, Azure DDoS Protection o Akamai Kona Site Defender. Questi servizi offrono protezione specifica contro vari tipi di attacchi DDoS.

- **Load Balancing**:
  Implementare il bilanciamento del carico (load balancing) per distribuire il traffico tra più server, migliorando la resilienza e riducendo il rischio che un singolo server venga sopraffatto. La resilienza di un server si riferisce alla sua capacità di continuare a funzionare correttamente e di recuperare rapidamente in caso di guasti, attacchi ecc...
  In altre parole, un server resiliente è progettato per essere robusto e per mantenere la disponibilità e l'integrità dei servizi anche di fronte a imprevisti. La resilienza è un aspetto cruciale della progettazione e della gestione delle infrastrutture IT, specialmente per servizi critici come quelli di e-commerce.

- **Scalabilità Automatica (Auto-Scaling)**:
  Configurare l'infrastruttura per scalare automaticamente in risposta a picchi di traffico. Esistono servizi che possono aiutare a gestire improvvisi aumenti di traffico. L'Auto-Scaling è una tecnica fondamentale per migliorare la resilienza delle applicazioni web contro gli attacchi DDoS. Questa tecnologia consente di adattare automaticamente le risorse del server in risposta alle variazioni del carico di lavoro monitorando continuamente le metriche di utilizzo delle risorse, come CPU, memoria, traffico di rete e numero di richieste al server. Quando viene rilevato un aumento del carico (che potrebbe essere dovuto a un attacco DDoS), il sistema di auto-scaling aggiunge automaticamente istanze di server per distribuire il carico

- **Firewall e Intrusion Detection Systems (IDS)**:
  Utilizzare firewall e IDS/IPS (Intrusion Prevention Systems) avanzati per monitorare e filtrare il traffico dannoso. Configurare regole specifiche per bloccare i pattern di traffico tipici degli attacchi DDoS.

- **Rate Limiting e Throttling**:
  Implementare politiche di rate limiting e throttling per limitare il numero di richieste che un singolo indirizzo IP può fare in un certo intervallo di tempo. Questo può aiutare a mitigare gli attacchi che tentano di sopraffare il sistema con richieste massicce.

- **Anycast Routing**:
  Utilizzare Anycast routing per distribuire il traffico a più data center. Questo aiuta a disperdere il traffico DDoS su più punti di ingresso, rendendo più difficile per l'attaccante sopraffare la rete. **Anycast routing** è una tecnica di routing di rete in cui lo stesso indirizzo IP viene assegnato a più nodi (server o dispositivi) situati in diverse posizioni geografiche. Quando un client invia una richiesta a questo indirizzo IP, la rete instrada automaticamente la richiesta al nodo più vicino o al nodo più accessibile in base a criteri come la distanza geografica, il numero di salti di rete o la latenza.

- **Monitoraggio e Alerting**:
  Implementare strumenti di monitoraggio e sistemi di allerta per rilevare e rispondere rapidamente agli attacchi DDoS. Rilevare e rispondere rapidamente a questo tipo di attacchi è cruciale per un e-commerce per diverse ragioni che riguardano la continuità operativa, la reputazione, la sicurezza dei dati e l'impatto finanziario.

In conclusione, accorgersi e agire rapidamente agli attacchi DDoS è vitale per ogni e-commerce, per garantire la continuità operativa, proteggere la reputazione del marchio, minimizzare l'impatto finanziario, salvaguardare i dati dei clienti e rispettare le normative di sicurezza.

RESPONSE

In ambito di response, prendendo in ipotesi che l'applicazione Web venga infettata da un malware e la nostra priorità sia che il malware non si propaghi sulla nostre rete, mentre non siamo interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata, la strategia deve concentrarsi sull'isolamento della macchina compromessa e sulla protezione del resto della rete.

Schema delle azioni da intraprendere per l'isolamento della macchina infetta dalla rete:

- **Disconnettere dalla Rete Interna**: Rimuovere la macchina infettata dalla rete interna per evitare che il malware si propaghi ad altri sistemi. Questo può essere

fatto fisicamente scollegando il cavo di rete o disabilitando l'interfaccia di rete tramite software.

- **Creare una VLAN Isolata**: Se la macchina deve rimanere connessa per il monitoraggio, spostarla in una VLAN isolata senza accesso ad altre parti della rete. Questo consente di osservare l'attività del malware senza rischiare ulteriori infezioni.
- **Utilizzare IDS/IPS**: Configurare sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS) per monitorare il traffico proveniente dalla macchina infettata e identificare attività sospette.
- **Restrizioni delle Policy di Sicurezza**: Applicare policy di sicurezza restrittive tramite il firewall e il sistema operativo per limitare la capacità del malware di comunicare o eseguire azioni dannose.
- **Controllo degli Accessi**: Configurare il controllo degli accessi per impedire alla macchina infettata di accedere a risorse critiche della rete.
- **Micro-segmentazione**: Implementare micro-segmentazione della rete per ridurre la superficie di attacco e isolare ulteriormente le risorse critiche.
- **Zero Trust Network**: Adottare un modello di sicurezza Zero Trust, in cui ogni richiesta di accesso è verificata e autenticata, indipendentemente dalla provenienza interna o esterna.
- **Network Access Control (NAC)**: Implementare soluzioni NAC per controllare e gestire l'accesso alla rete basato sullo stato di sicurezza degli endpoint.

In conclusione l'approccio descritto consente di impedire la propagazione del malware nella rete, mantenendo al contempo il monitoraggio della macchina infettata per analizzare il comportamento del malware e raccogliere informazioni utili per future azioni di mitigazione e prevenzione. L'implementazione di misure di isolamento, monitoraggio e contenimento, insieme a soluzioni di sicurezza avanzate, garantisce una risposta efficace all'incidente senza compromettere la sicurezza complessiva della rete.