W20D4

Giacomo di Giacinto

EPICODE

Esercizio
Traccia e requisiti

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**

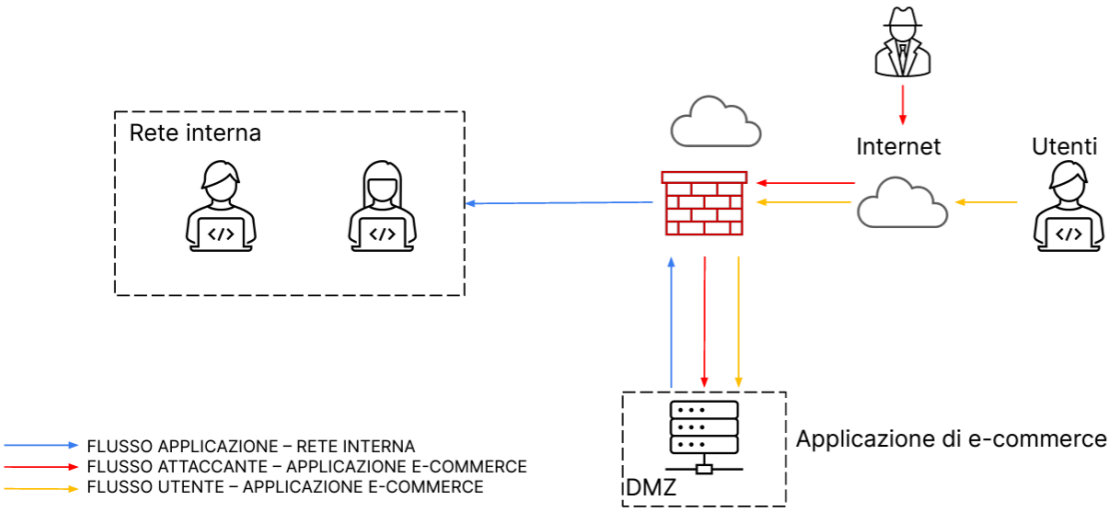
3. **Response**: l'applicazione Web viene infettata da un malware.
   La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata.
   Modificate la figura in slide 2 con la soluzione proposta.

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.

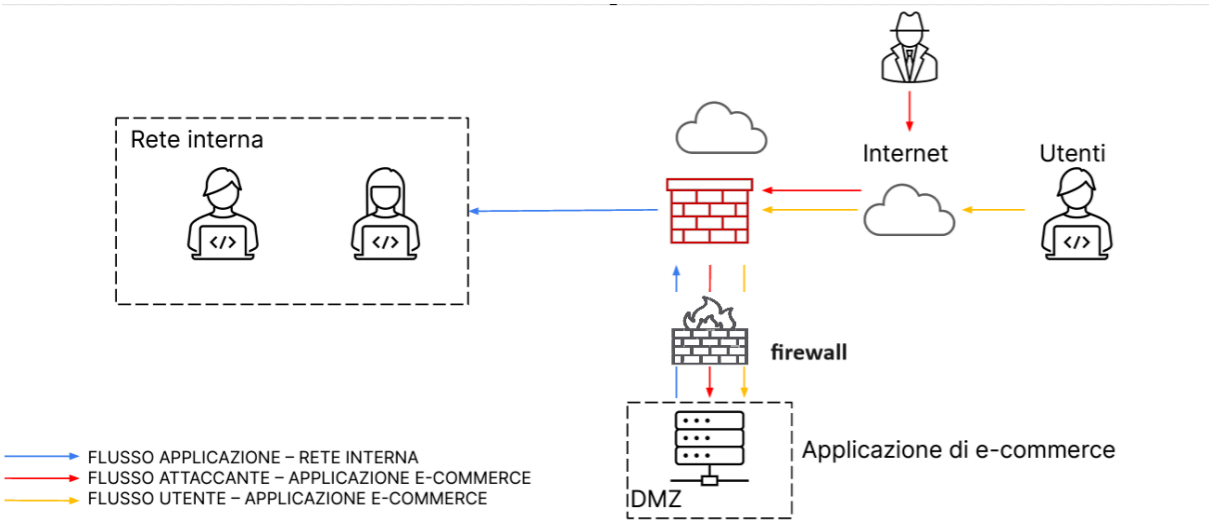
La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.



1)

Le misure preventive per proteggere un'applicazione web da attacchi SQL injection (SQLi) e cross-site scripting (XSS) possono includere:

- **Implementazione di un Web Application Firewall (WAF)**: posizionato davanti all'applicazione di e-commerce, il WAF filtra e blocca richieste malevole che contengono payload SQLi e XSS. Agisce come una barriera di protezione, controllando gli accessi alle risorse del sistema e filtrando tutto il traffico tra l'ambiente interno e quello esterno. Un WAF è specializzato nell'intercettare e analizzare il traffico HTTP, e può adottare un modello di sicurezza positivo (consentendo solo transazioni valide) o analitico (analizzando ogni messaggio alla ricerca di minacce e confrontandolo con database noti per inserirlo in white o black list). I WAF di ultima generazione, denominati 3.0, sono in grado di prevenire attacchi specifici, identificare vulnerabilità e ricostruire la catena degli eventi durante sessioni particolari.
- **Validazione e sanitizzazione degli input utente**: garantire che l'applicazione esegua controlli adeguati sugli input degli utenti prima di utilizzarli nelle query o negli output HTML.
- **Aggiornamenti e patch di sicurezza**: applicare regolarmente patch di sicurezza e aggiornamenti software per proteggere dalle vulnerabilità note.
- **Protezione contro HTTP CSRF (cross-site request forgery)**: abilitare meccanismi di difesa per proteggere i siti web da richieste non autorizzate, assicurandosi che ogni richiesta sia inviata intenzionalmente dal client.



2)

Per quanto riguarda la protezione da attacchi DDoS (Distributed Denial of Service), considerando l'impatto economico di un attacco di 10 minuti che potrebbe causare una perdita di 15.000€ (10 minuti * 1.500€/minuto), le azioni preventive possono includere:

- **Soluzioni anti-DDoS**: implementare servizi cloud o dispositivi dedicati per mitigare gli attacchi DDoS.
- **Capacità di banda e scalabilità**: assicurarsi di avere una banda sufficiente e una capacità di scalabilità per gestire i picchi di traffico.
- **Configurazione di firewall e sistemi di rilevamento delle intrusioni**: configurare correttamente questi sistemi per bloccare il traffico malevolo.

Adottare queste misure preventive può significativamente ridurre il rischio di attacchi informatici e minimizzare l'impatto economico e operativo sul business

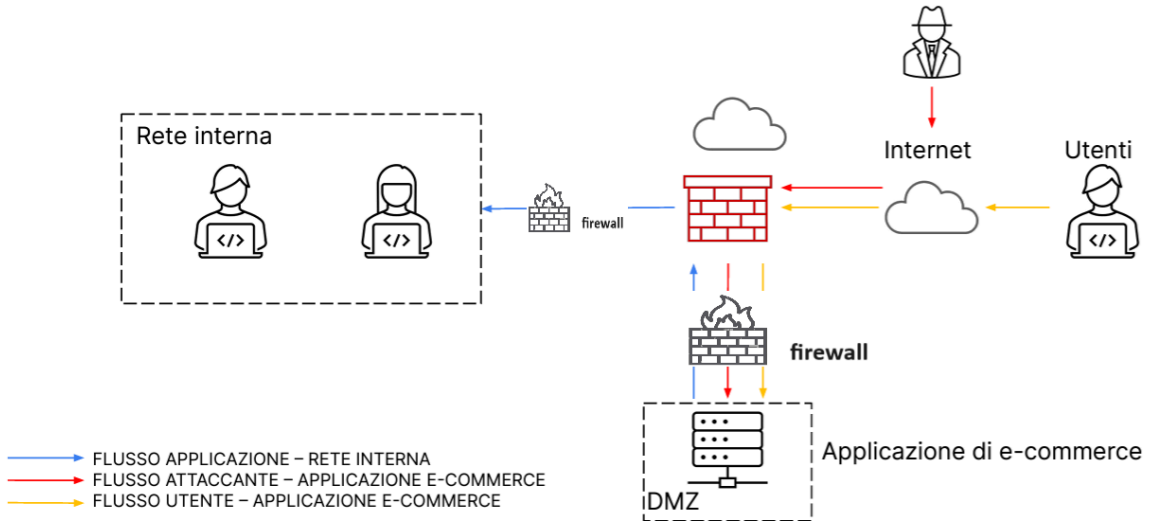
3)

Per evitare la diffusione di un malware dannoso nella rete interna, una soluzione efficace è isolare il server web compromesso dalla DMZ utilizzando un firewall dedicato che blocchi tutte le connessioni in ingresso e uscita, tranne il traffico legittimo verso Internet per l'e-commerce.

In dettaglio, questa soluzione include i seguenti elementi:

- **Isolamento del server dell'applicazione di e-commerce**: Il server è collocato nella DMZ (zona demilitarizzata) e isolato tramite un firewall dedicato, che blocca tutte le comunicazioni indesiderate provenienti dal server, nel caso in cui venga compromesso. Questo firewall permette solo il traffico necessario per il funzionamento dell'e-commerce, riducendo il rischio di propagazione del malware.
- **Protezione della rete interna aziendale (LAN)**: La rete interna è protetta da un sistema IPS/Firewall, che impedisce qualsiasi attacco proveniente dalla DMZ isolata, bloccando potenziali propagazioni di malware o accessi non autorizzati. Questo livello di sicurezza aggiuntivo assicura che, anche se un server nella DMZ viene compromesso, il malware non possa infiltrarsi nella rete interna.

Questa infrastruttura protegge sia a livello dell'applicazione web che a livello di rete, isolando efficacemente eventuali compromissioni e limitando i danni a quel segmento specifico.



Per migliorare ulteriormente la sicurezza, si potrebbe:

- **Migrare l’applicazione e-commerce su un cloud dedicato e isolato**: Separare l'applicazione e-commerce dalla rete aziendale e ospitarla su un ambiente cloud dedicato. Questo approccio garantisce che, anche in caso di compromissione, l'attaccante non possa raggiungere la rete interna aziendale. La gestione amministrativa dell'applicazione dovrebbe essere effettuata tramite accesso VPN o sistemi simili, garantendo che solo il personale autorizzato possa accedere alle risorse del cloud.

Queste misure preventive rafforzano la sicurezza complessiva dell'infrastruttura, proteggendo l'applicazione e-commerce da attacchi e impedendo la propagazione di minacce all'interno della rete aziendale.