PROGETTO W20D4

EPICODE

Esercizio
Traccia e requisiti

Traccia:

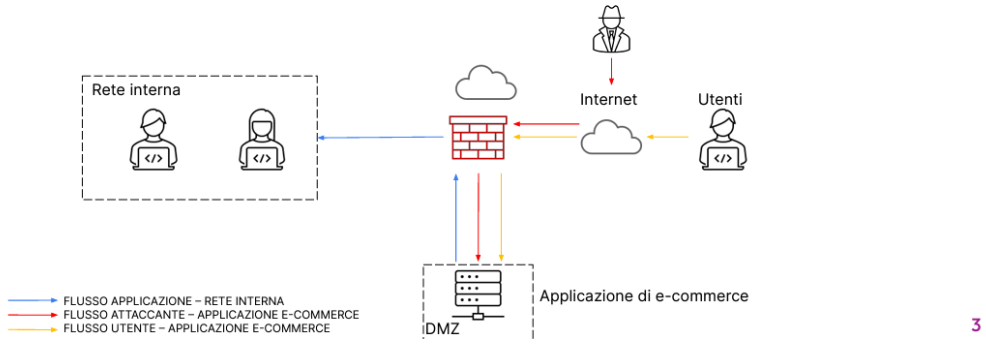
Con riferimento alla figura in slide 2, rispondere ai seguenti quesiti.

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)**

2

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

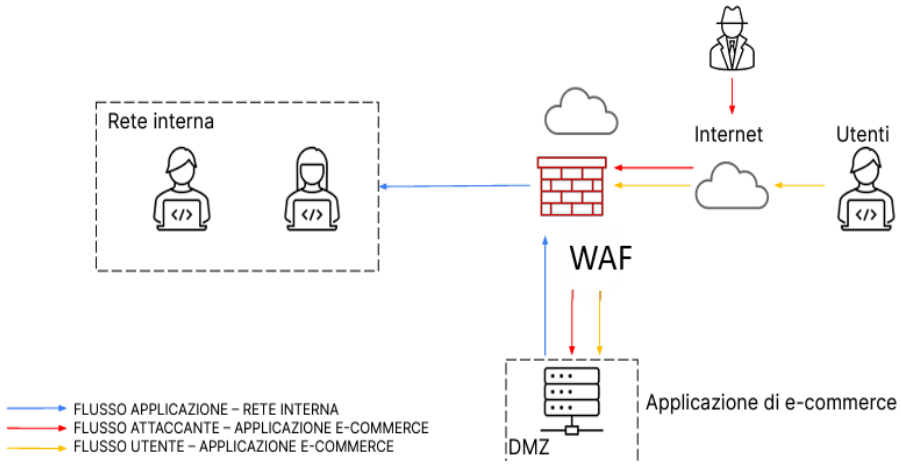
La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.



3

1- Quando si tratta di proteggere le Web App da minacce come XSS e SQL Injection, una soluzione preventiva efficace è l'implementazione di un Web Application Firewall (WAF). A differenza dei firewall tradizionali, i quali sono progettati principalmente per controllare il traffico di rete generale, i WAF sono specificamente progettati per proteggere le Web App da attacchi mirati come XSS e SQLi. (WAF) è essenziale per proteggere le Web App da minacce come XSS e SQLi. Il WAF viene posizionato tra gli utenti e la Web App, agisce come uno scudo protettivo che filtra il traffico in entrata, rilevando e bloccando tentativi di

exploit, fornendo una barriera efficace contro attacchi noti e sconosciuti.

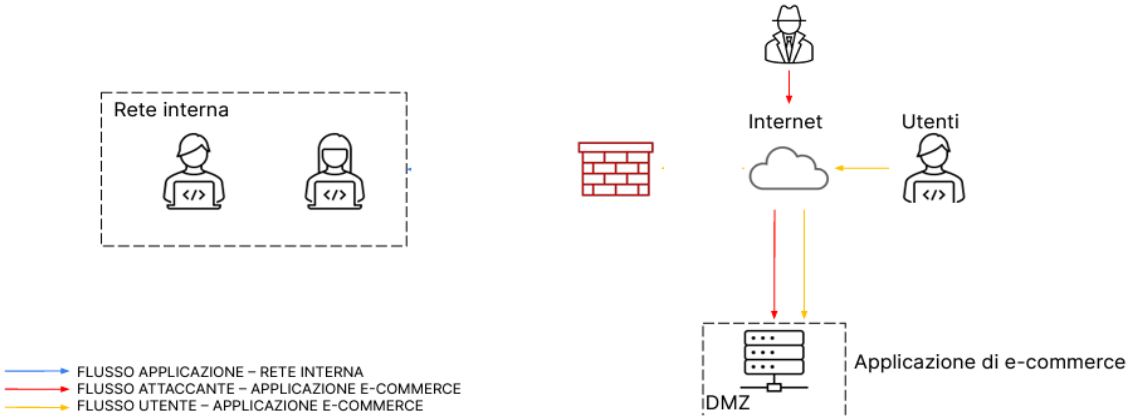


2- Considerando una perdita di €1 500 al minuto per l'inattività del servizio durante un attacco DDoS che rende il servizio non disponibile per 10 minuti, si stima una perdita totale di circa €15 000. L'attacco di tipo DDoS causa la non raggiungibilità della piattaforma di e-commerce per 10 minuti. Considerando che gli utenti spendono circa 1.500€ al minuto, possiamo stimare i danni causati dal mancato guadagno sul business moltiplicando la spesa potenziale degli utenti per minuto (1.500€) per i minuti di indisponibilità del servizio (10). Di conseguenza, l'impatto sul business è di €15 000, ovvero per 10 minuti di indisponibilità la compagnia ha perso €15 000 di acquisti potenziali.

   Per prevenire gli attacchi DDoS, ci sono diverse azioni consigliate. Una di queste è l'implementazione di un Web Application Firewall (WAF), che è efficace nel rilevare e mitigare il traffico dannoso, come già detto nella soluzione precedente. Un’alta azione consigliata potrebbe essere l’aggiunta di un Load Balancer, distribuendo il traffico su più server backend, riducendo così il carico su ciascun server e mitigando l'impatto dell'attacco.

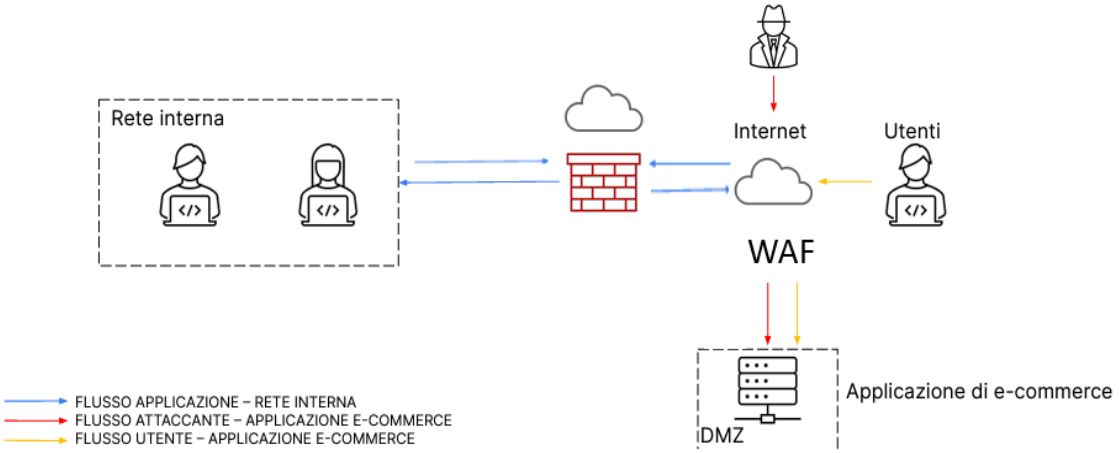
3- <u>L'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostra rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata.</u>

È possibile implementare una strategia focalizzata sull'isolamento della macchina infettata. Ciò comporta il collegamento diretto della macchina a Internet, rendendola accessibile agli attaccanti ma disconnessa dalla rete interna.



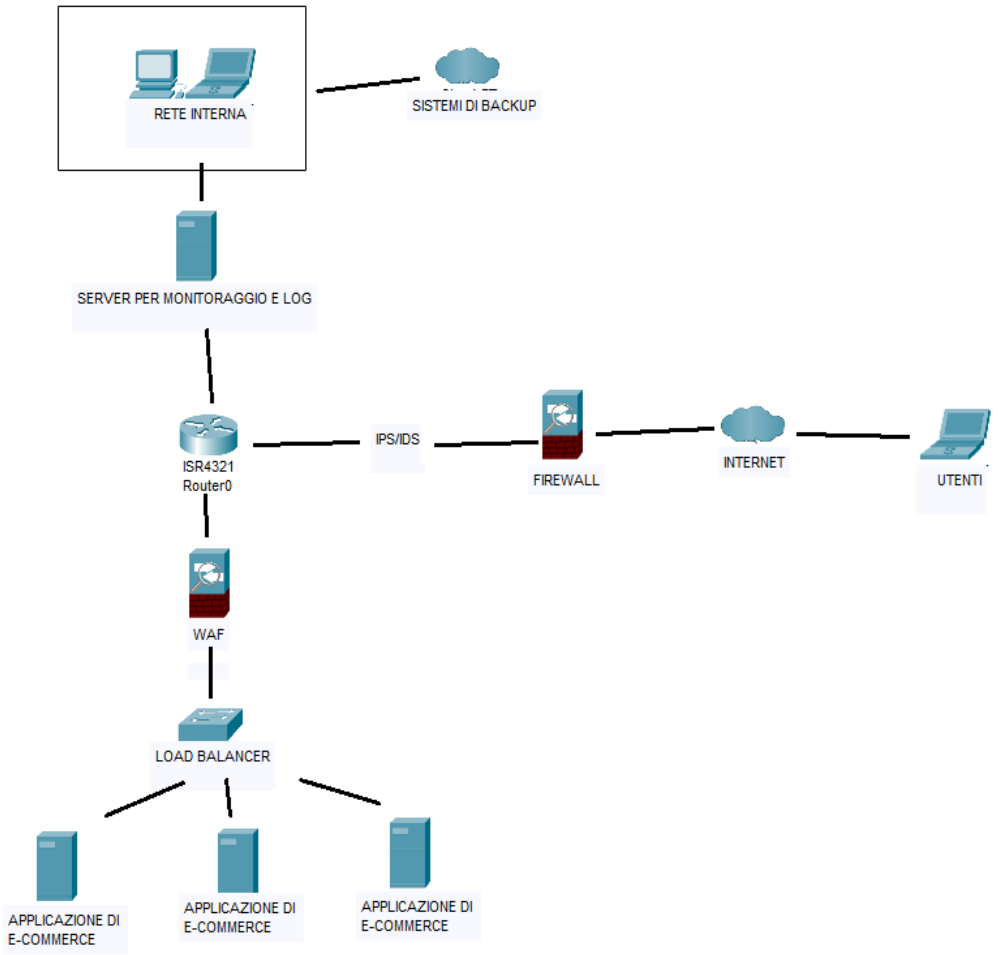
3

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



3

5- Modifica più aggressiva dell'infrastruttura:



Questa è la mia proposta di modifica dell'infrastruttura. Come si può vedere dalla figura sopra ho aggiunto anche altri sistemi per la sicurezza come:

- Firewall con IPS/IDS (Intrusion Prevention System/Intrusion Detection System): Questo firewall avanzato è dotato di funzionalità IPS e IDS per individuare e prevenire attivamente gli attacchi. Monitora il traffico in tempo reale per identificare potenziali minacce e intrusi, e intraprende azioni immediate per bloccarli.

- Load Balancer: l’aggiunta di un bilanciatore di carico tra il server dell'applicazione di e-commerce e gli utenti esterni migliora la disponibilità e la scalabilità del servizio. Inoltre, fornisce una difesa aggiuntiva contro gli attacchi DDoS, distribuendo equamente il carico del traffico in entrata e prevenendo sovraccarichi che potrebbero compromettere l'integrità del servizio.
- Server per Monitoraggio e Log: Questi server sono dedicati al monitoraggio continuo della sicurezza della rete e alla registrazione degli eventi di sistema. Raccolgono dati sul traffico di rete, le attività degli utenti e gli eventi di sicurezza, consentendo agli amministratori di sistema di identificare e rispondere prontamente a eventuali violazioni o anomalie di sicurezza.
- Sistemi di Backup: Questi sistemi sono responsabili della copia e del ripristino dei dati critici dell'infrastruttura, garantendo la disponibilità e l'integrità dei dati in caso di perdita o corruzione.