S9L5

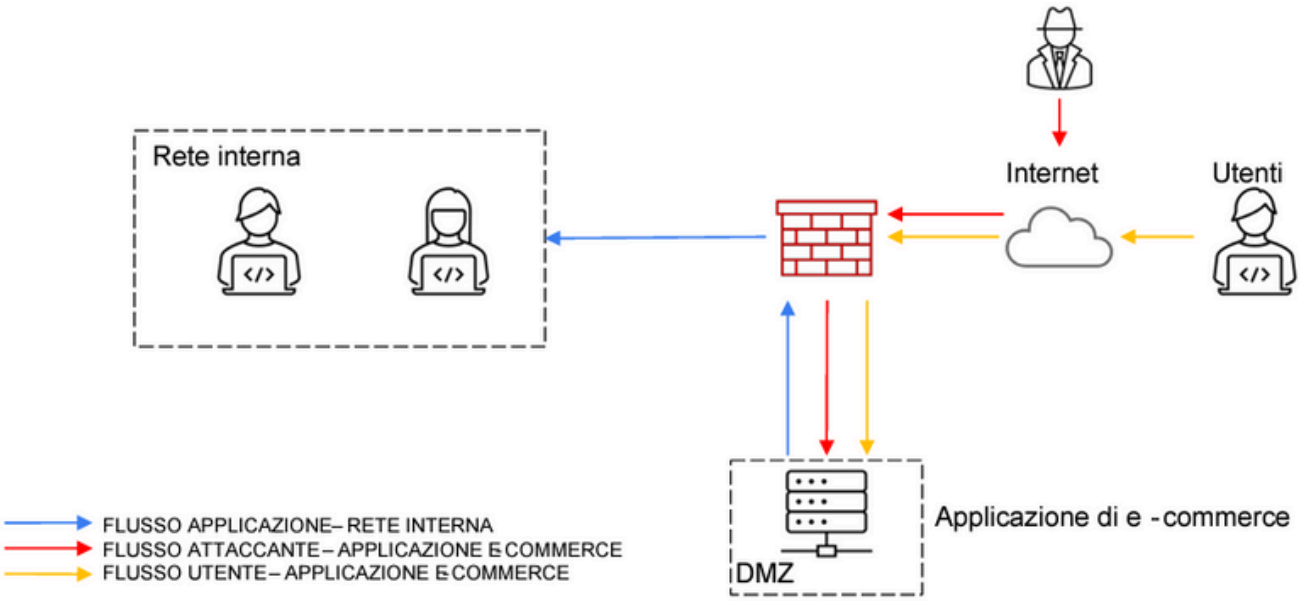
Sarah Ortiz

TRACCIA

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

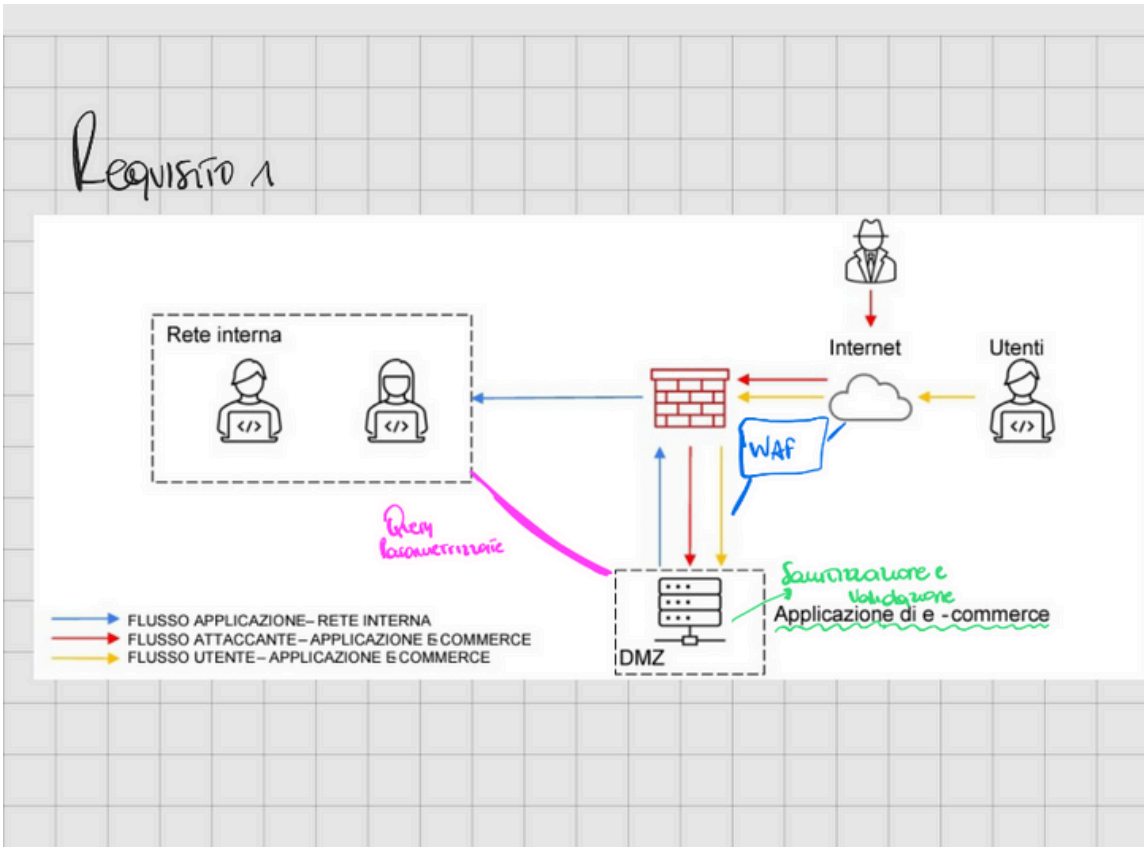
1. Azioni preventive : quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni. È richiesta sola modifica
2. Impatti sul business : l'applicazione Web subisce un attacco di tipo l'applicazione non raggiungibile per 10 minuti . DDoS dall'esterno che rende Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media minuto gli utenti spendono ogni 1.200 € 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: integrando eventuali altri elementi di sicurezza (integrando anche una soluzione al punto 2) Budget 5000-10000 euro. Eventualmente fare piu proposte di spesa

Architettura di rete:
l’applicazione di e-commerce deve essere disponibile per gli utenti tramite 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 attacante potrebbe raggiunger ela rete interna



AZIONI PREVENTIVE DA ATTACCHI DI TIPO SQLI E XSS

Per difendere l'applicazione dagli attacchi SQLi e XSS, sono state implementate diverse misure preventive. Prima di tutto, le query SQL sono state parametrizzate per prevenire l'inserimento di comandi SQL malevoli. Dopodiche, è stata aggiunta la validazione e sanitizzazione degli input degli utenti, riducendo così la possibilità che input dannosi raggiungano il database o vengano eseguiti come codice.



IMPATTI SUL BUISNESS

Un attacco ddos può avere impatti significativi sul business. Se l'applicazione di ecommerce diventa non raggiungibile per 10 minuti, e considerando che gli utenti spendono mediamente 1.200 € al minuto, l'impatto economico sarà di 12.000 €.
Formula per calcolare l’impatto economico=1.200 €×10 minuti=12.000 €

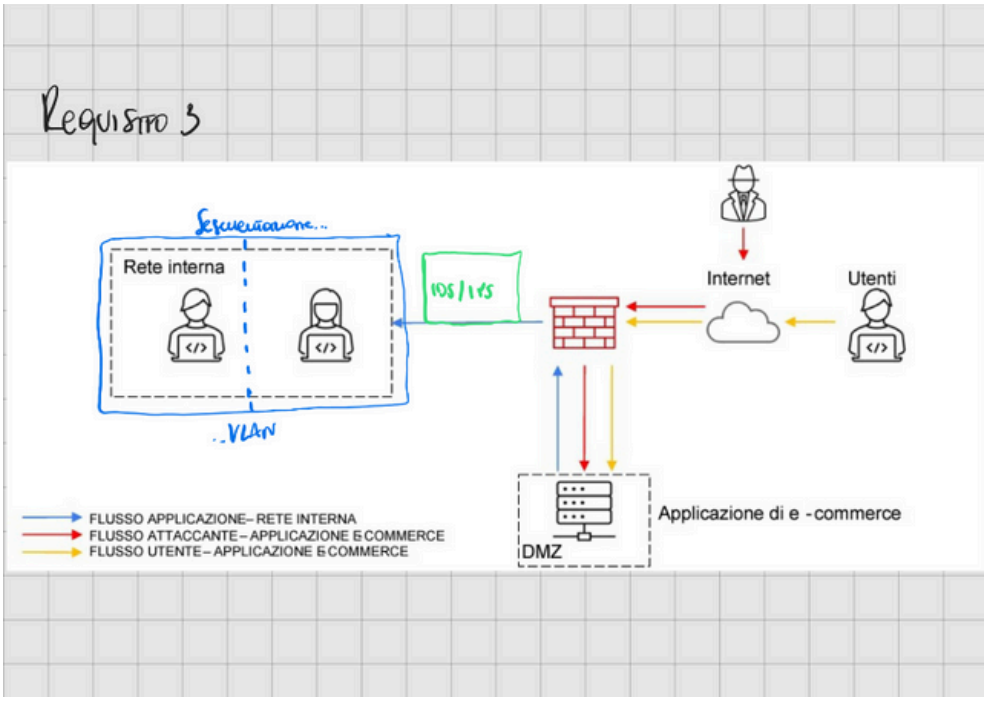
Perdita di ricavi=Tasso di entrate per minuto (euro) ×Tempo di inattività (min)

Calcolare l'impatto economico di un attacco ddos è essenziale per comprendere l'importanza di investire in misure preventive. La perdita di €12.000 per 10 minuti di inattività evidenzia la necessità di protezioni per garantire la continuità del servizio di ecommerce

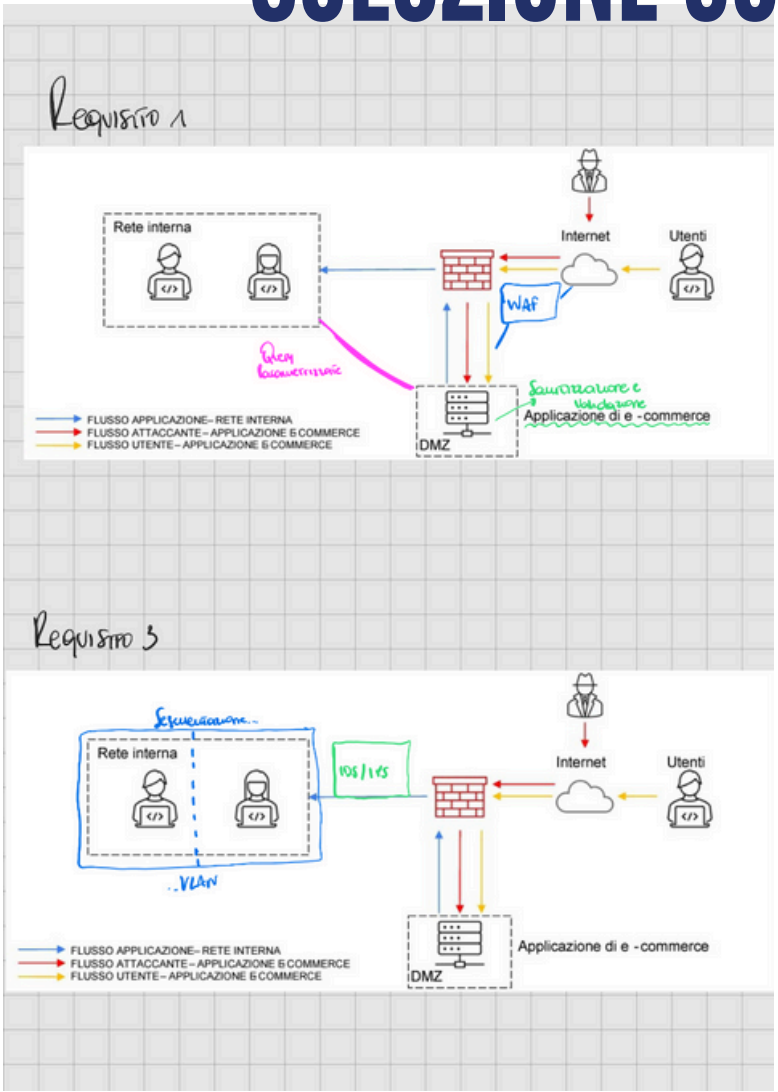
RESPONSE

Obiettivi:

- Impedire la propagazione del malware nella rete interna.
- Isolare la macchina infettata utilizzando segmentazione della rete (VLAN).
- Sistema di rivelamento delle intrusioni, è il processo di monitoraggio del traffico di rete e di analisi dei segnali di possibili intrusioni, come tentativi di exploit e incidenti che potrebbero costituire una minaccia imminente per la rete (IDS/IPS)



SOLUZIONE COMPLETA



- La validazione e la sanitizzazione degli input sono state integrate nell'applicazione ecommerce.
- Il WAF è stato posizionato tra Internet e il firewall principale per bloccare attacchi noti.
- Il firewall è stato inserito tra la DMZ e la rete interna per prevenire la propagazione del malware.
- I IDS/IPS sono stati messi tra la rete interna e il firewall per monitorare il traffico e rilevare eventuali attività sospette.

MODIFICA PIÙ "AGGRESSIVA" DELL'INFRASTRUTTURA

Misure di sicurezza	
WAF	
Sanitizzazione e validazione	
Query parametrizzate	
Segmentazione VLAN	
IDS/IPS	
budget stimato	5000-10000

Queste misure migliorano la sicurezza dell'infrastruttura dell'applicazione di e-commerce, garantendo una protezione più robusta contro vari tipi di attacchi e minimizzando l'impatto economico di eventuali compromissioni.