Esercizio S9 L5

Traccia:

Con riferimento alla figura in slide 3, rispondere ai seguenti quesiti.

1. Azioni preventive:

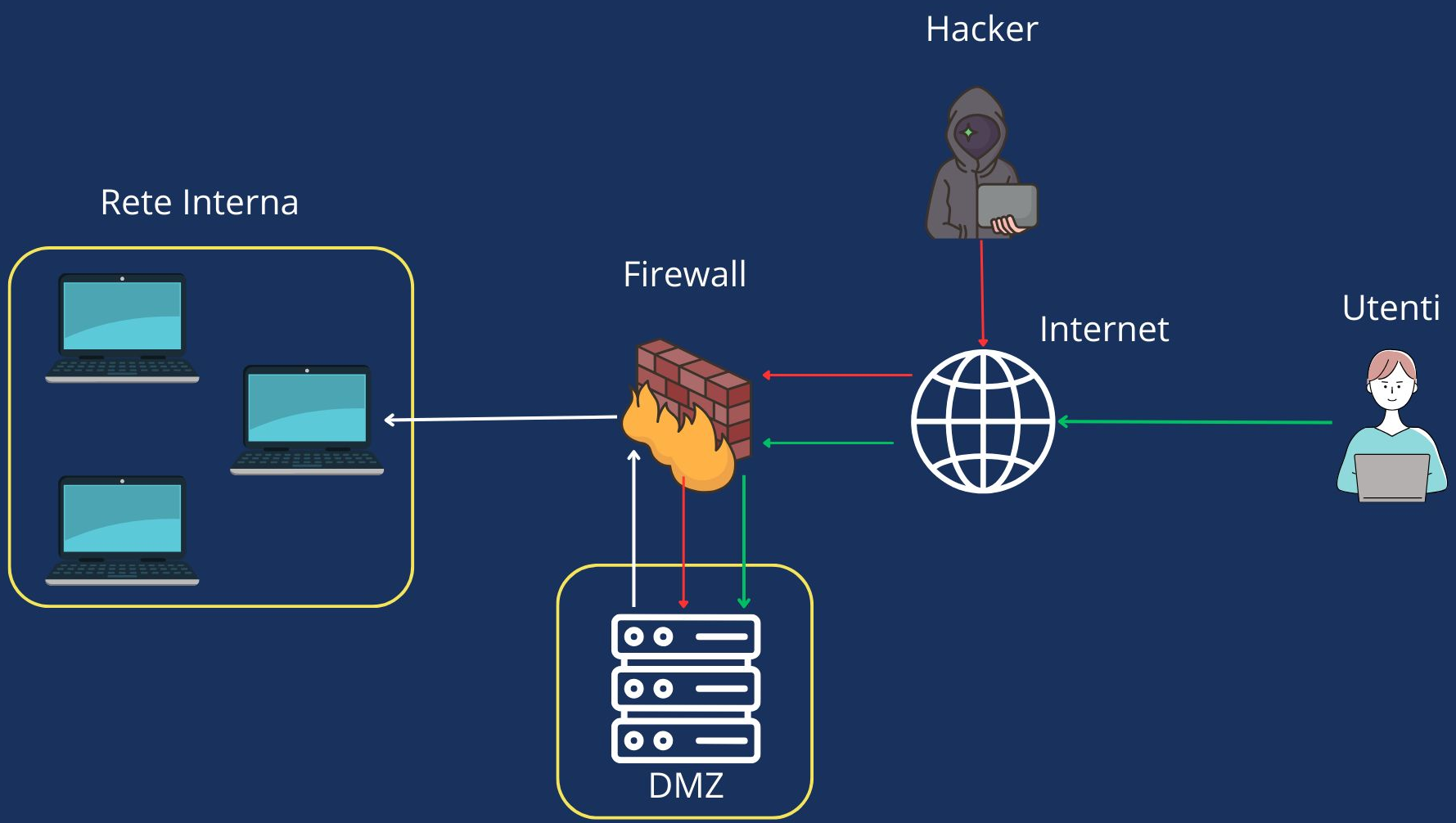
Quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni.

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.

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.

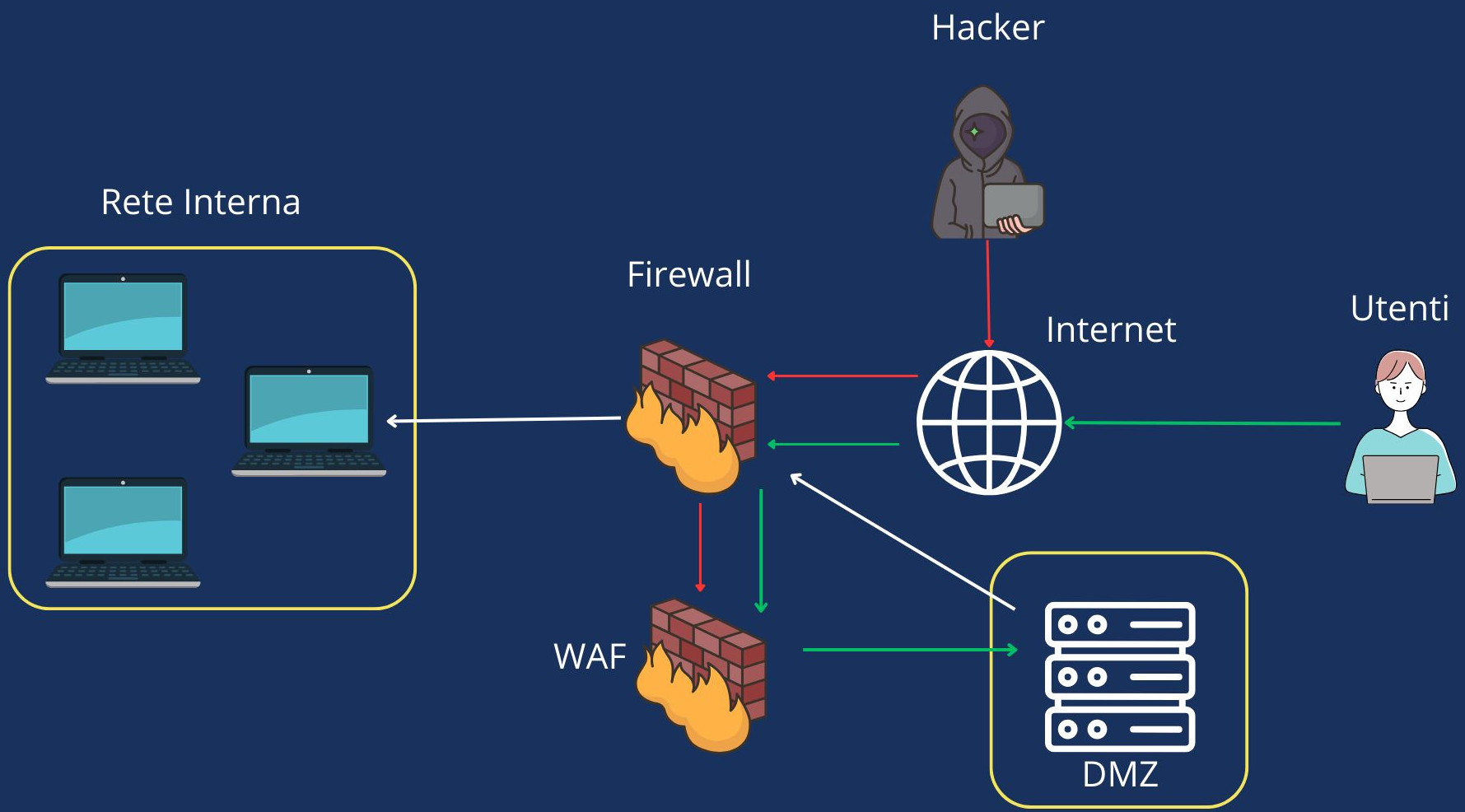

Hacker
Rete Interna
Firewall
Internet
Utenti
DMZ

Azioni preventive: prevenire attacchi di tipo XSS e SQLi

Generalmente il miglior modo per prevenire attacchi XSS, SQLi ed in generale qualsiasi tipo di attacco alle Web App è di implementare un WAF, ovvero un Web Application Firewall ben configurato che monitora il traffico e limita le richieste inviate alle applicazioni così da permettere l'accesso solamente agli utenti legittimi.

Altri metodi per prevenire vari tipi di attacchi alle Web App sono l'implementazione delle Best Practices di sicurezza nella scrittura del codice che fa girare la Web App in sè e che mitigano e talvolta impediscono completamente la possibilità di effettuare determinati tipi di attacchi.

Vediamo adesso come implementare un WAF nella configurazione precedente.


Hacker
Rete Interna
Firewall
Internet
Utenti
WAF
DMZ

Impatti sul business: stima dei danni

Il secondo quesito esamina la situazione in cui la Web App viene contrassegnata come bersaglio di un attacco DDoS, ovvero un Distributed Denial of Service, una tipologia di attacco coordinato dove molteplici macchine inviano contemporaneamente grandi quantità di pacchetti allo stesso indirizzo IP, generando una enorme quantità di traffico con l'obiettivo di intasare la rete ed impedire il corretto funzionamento del servizio. Nel nostro caso l'attacco è riuscito ad impedire il corretto funzionamento per 10 minuti. Sappiamo anche che gli utenti spendono in media 1500 € al minuto.

Calcolare il guadagno perso è facile in questo caso sarà sufficiente moltiplicare il denaro al minuto perso per il numero di minuti che il servizio non è stato raggiungibile.

1.500 x 10 = 15.000 €

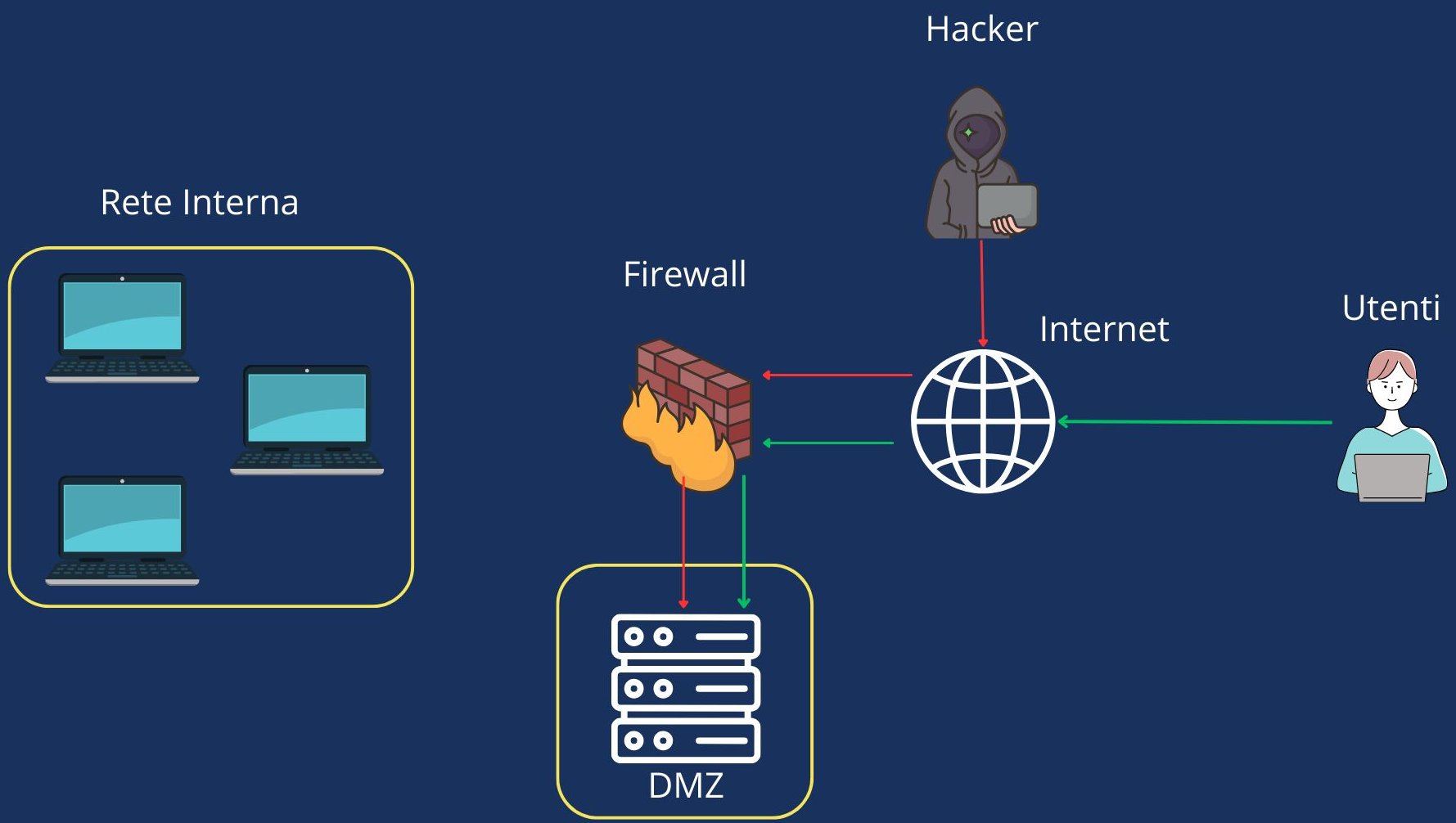
La stima finale dei danni economici per l'azienda sarà di 15.000 €

Response: salvaguardia della rete interna

Nello scenario proposto L'applicazione Web viene infettata da un malware e dobbiamo fare in modo che non si propaghi sulla rete interna. Ci viene anche detto che possiamo lasciare il servizio infetto raggiungibile su internet.

Per fare ciò provvederemo a segmentare la rete seguendo i principi dell'isolamento e della rimozione del servizio infetto per fare in modo che i danni siano contenuti, procediamo dunque a separare la rete interna dal resto dello schema di rete, così facendo ci assicuriamo che la rete interna diventi un ambiente isolato non raggiungibile da internet nè dalla Web App infetta.

Nelle prossime slides troviamo la configurazione di rete modificata per rappresentare quanto detto sopra.


Hacker
Rete Interna
Firewall
Internet
Utenti
DMZ