PROJECT MODULE 5

FATIMA NARDA NICOLETT RODRIGUEZ ORTEGA

1) TRACCIA

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**

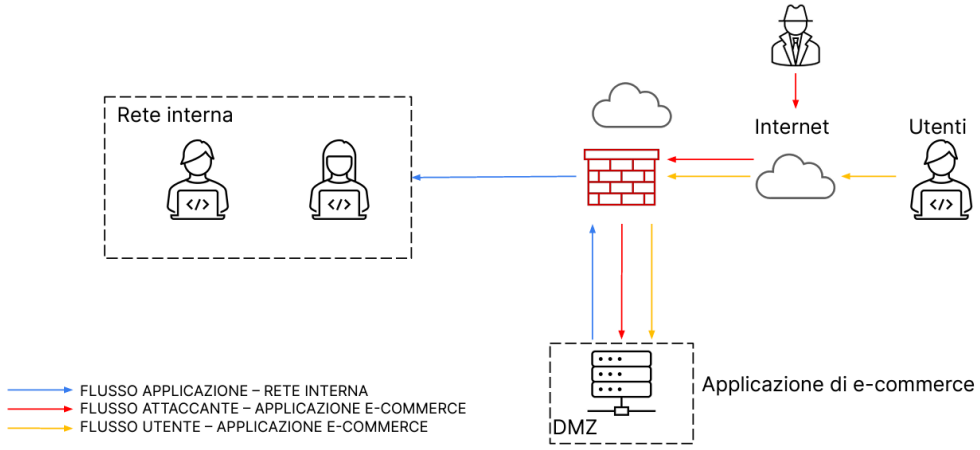
3. **Response**: l'applicazione Web viene infettata da un malware.
   La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata.
   Modificate la figura in slide 2 con la soluzione proposta.

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.

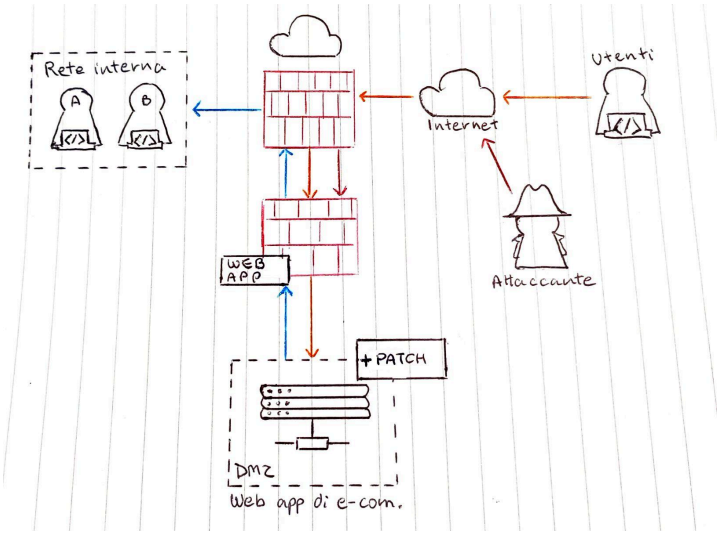
La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.



2) SVOLGIMENTO

I. Le misure da utilizzare per prevenire un SQL injection e un Cross Site Scripting da un attaccante sono l'implementazione di un Web Application Firewall, che è specializzato nella protezione di web app da tali attacchi; inoltre, l'applicazione regolare di patch può correggere le vulnerabilità esistenti, in

quanto esso introduce miglioramenti e aggiornamenti al codice e alla sicurezza della web app.

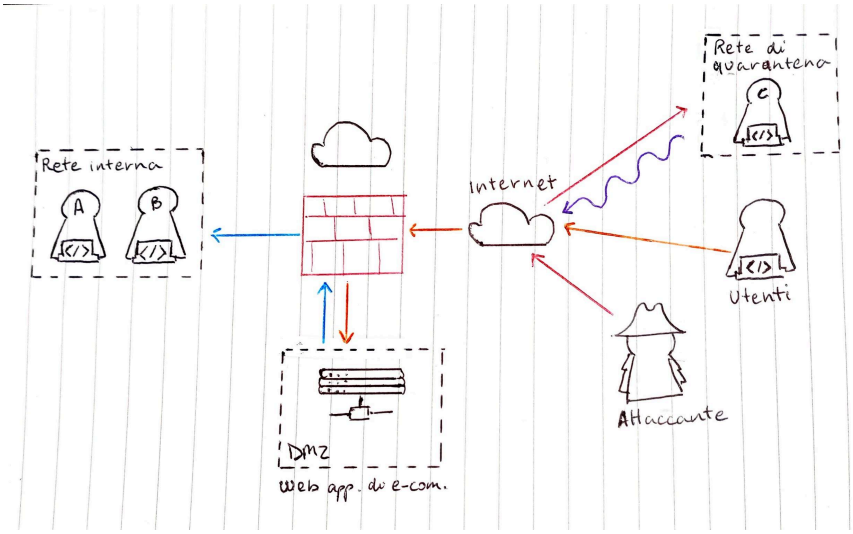


II. Calcolo impatto sul business:

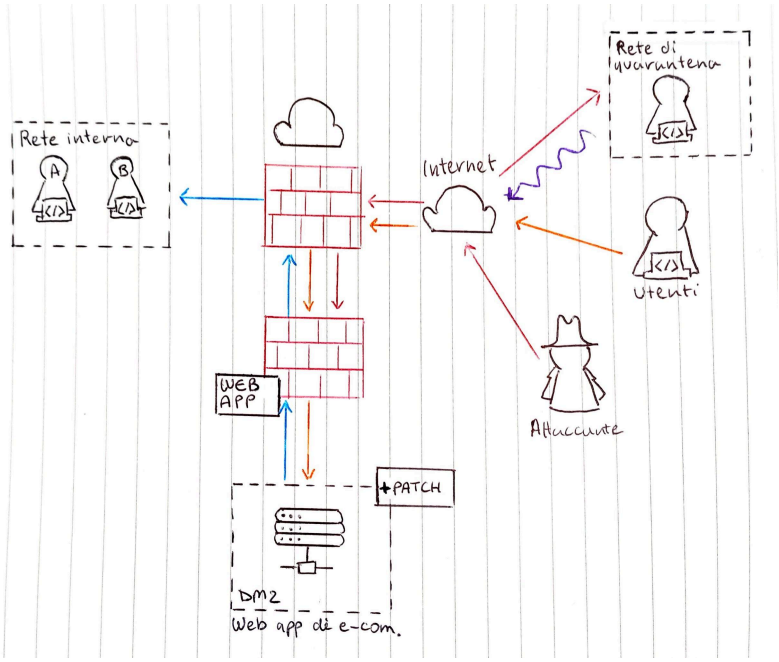
- Durata attacco = 10 minuti
- Guadagno medio al minuto = € 1.500,00
- Perdite totali = 10 * 1.500 = € 15.000,00

Il Network Access Control offre molti vantaggi per prevenire questo DDoS, esso consente di definire ed applicare regole rigide per controllare chi può accedere alle reti e quali risorse possono raggiungere, fornisce strumenti per il monitoraggio continuo rilevando anomalie.

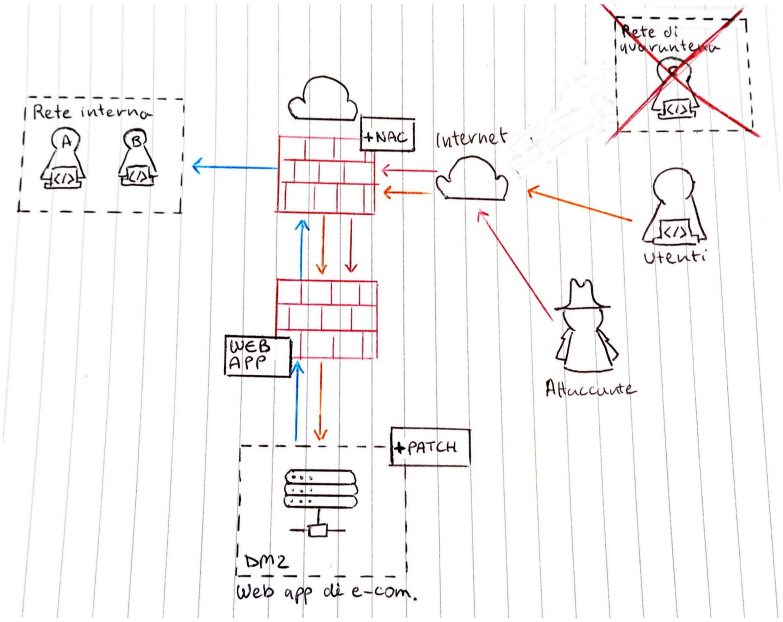
III. Per impedire che il malware si diffondi, bisogna isolare la macchina infetta in una rete di quarantena, disconettendola completamente dalla rete interna e collegandola ad Internet. L'attaccante ha ancora accesso alla macchina infetta e isolata, ma non alle macchine all'interno della rete interna.



IV.


Rete di quarantena
Rete interna
A
B
Internet
Utenti
WEB APP
Attaccante
+PATCH
DMZ
Web app di e-com.

V.


Rete di quarantena
Rete interna
A
B
+NAC
Internet
Utenti
WEB APP
Attaccante
+PATCH
DMZ
Web app di e-com.