Beatrice Folino

[M5 - Progetto Finale]

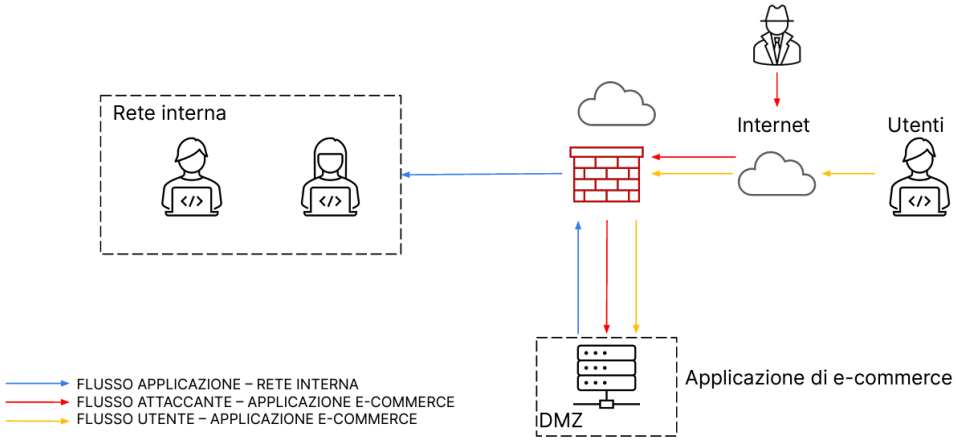
EPICODE - CYBERSECURITY CLASS

23 marzo 2024

In base all'immagine di seguito riproposta, vengono poste delle domande allo studente, si procederà quindi per step.

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.



QUESITO n.1 E SVOLGIMENTO

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.

In caso di attacchi SQLi e XSS possiamo prevedere una serie di azioni mirate.

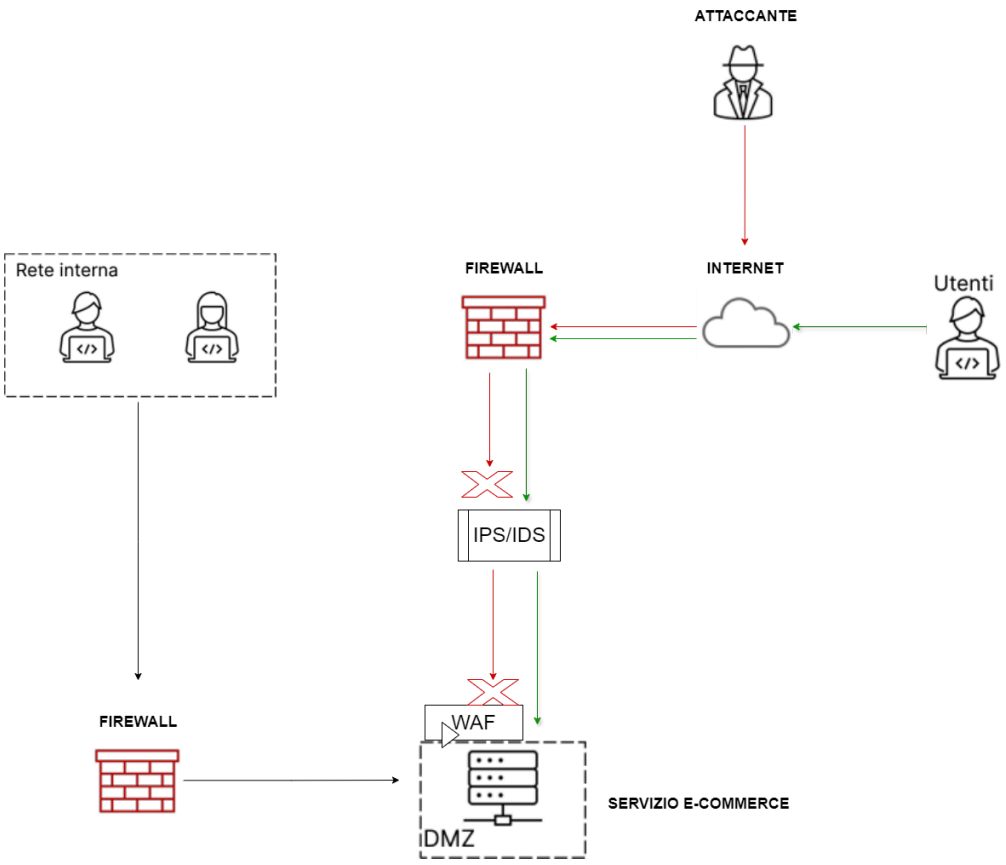
1. FILTRARE LE CONNESSIONI in ingresso in modo da identificare e neutralizzare eventuali user malevoli.

Il filtraggio può avvenire tramite:

- WAF (Web Application Firewall) direttamente su web app
- sull'intera rete aggiungendo IPS / IDS

2. CONTROLLI SUL SOFTWARE
   al fine di individuare bug nei software di gestione di DB.
   Ciò è possibile tramite:

- sanificazione del codice in modo da identificare eventuali caratteri speciali che consentono più facilmente attacchi di tipo SQL injection (esempio: validazione input e analisi statica del codice)
- reverse engineering per accedere al codice sorgente in modo da limitare processi XSS (esempio: analisi del codice sorgente e test di sicurezza della web app)



Nell'immagine sopra, è possibile vedere l'applicazione di WAF e sistemi IPS/IDS, che si interpongono tra la web app e l'attaccante, nonché l'aggiunta di un firewall ad hoc per la rete interna, per limitare ancor meglio il traffico di eventuali agenti esterni non autorizzati.

QUESITO n.2 E SVOLGIMENTO

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.

Per calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, possiamo moltiplicare il numero di minuti di indisponibilità per il valore medio generato dagli utenti sulla piattaforma di e-commerce per minuto.

Numero di minuti di indisponibilità: 10 minuti
Valore medio generato dagli utenti sulla piattaforma di e-commerce per minuto: 1.500 €

Impatto sull'attività = Numero di minuti di indisponibilità * Valore medio generato dagli utenti per minuto
Impatto sull'attività = 10 minuti * 1.500 €/minuto
Impatto sull'attività = 15.000 €

Quindi, l'impatto sull'attività dovuto alla non raggiungibilità del servizio per 10 minuti è di 15.000 €.

Per quanto riguarda le azioni preventive, ci sono diverse strategie che possono essere adottate per mitigare gli effetti di un attacco DDoS:

1. Utilizzo di un Web Application Firewall (WAF) per filtrare e mitigare il traffico DDoS in arrivo.
2. Utilizzo di servizi di mitigazione DDoS forniti da provider di servizi di rete.
3. Implementazione di un sistema di monitoraggio della disponibilità del servizio per rilevare rapidamente gli attacchi e rispondere prontamente.
4. Utilizzo di CDN (Content Delivery Network) per distribuire il traffico e mitigare gli effetti degli attacchi DDoS.
5. Implementazione di limitazioni di traffico e filtri IP per bloccare il traffico sospetto.

Queste sono solo alcune delle azioni preventive che possono essere adottate per affrontare gli attacchi DDoS e ridurre l'impatto sull'attività. È importante adottare una strategia di difesa multi-livello e personalizzata in base alle esigenze specifiche dell'organizzazione.

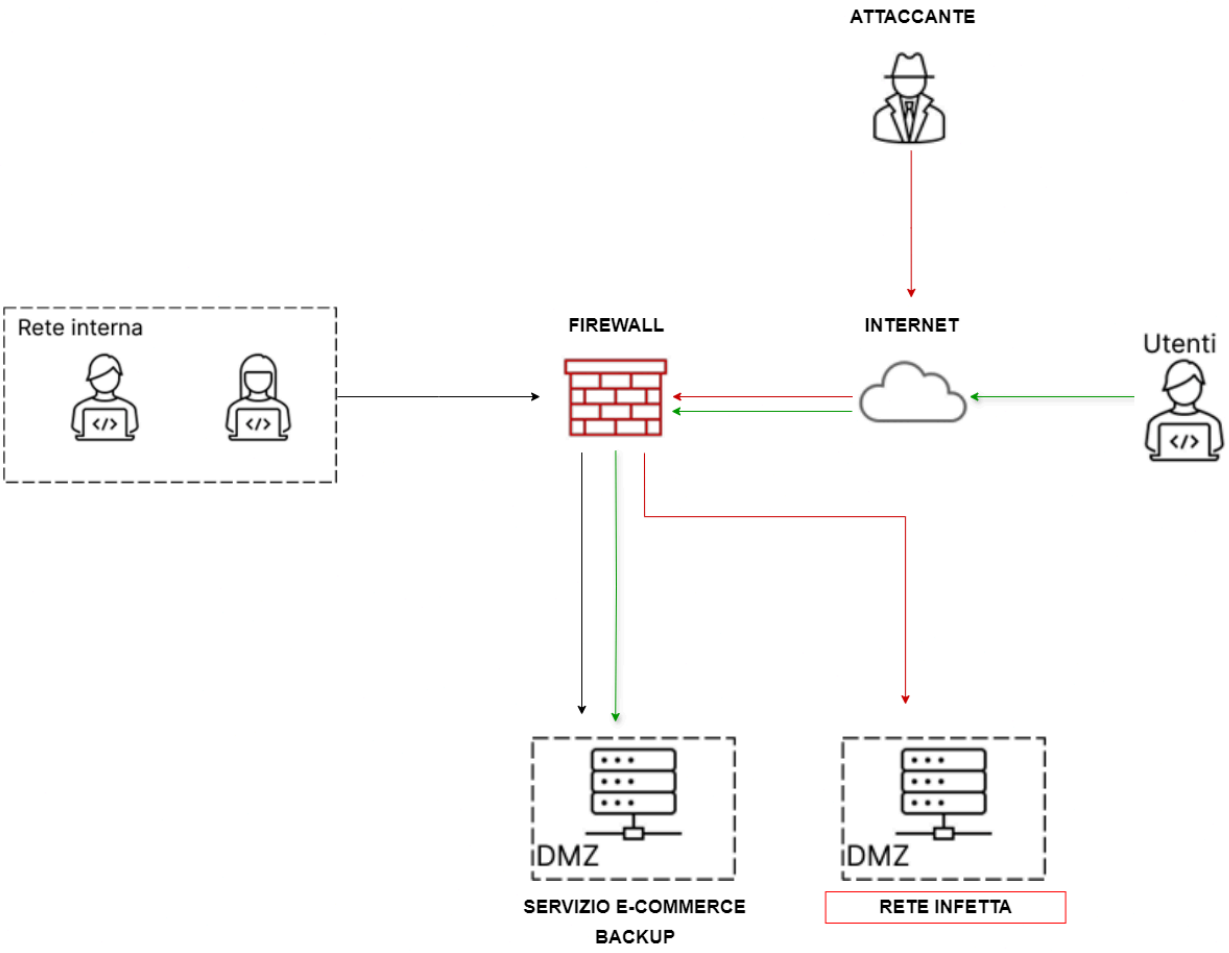
QUESITO n.3 E SVOLGIMENTO

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 con la soluzione proposta.

In questo caso, assumendo che esista un backup della web app, si procede con l'indirizzare il traffico dell'agente attaccante sulla rete/db che è già stata infettata, limitando lì la sua presenza.

Sul secondo server, quello di backup, avverrà invece il normale traffico previsto, ovvero le connessioni della rete interna e quelle degli utenti che devono usufruire dei servizi dell'ecommerce.

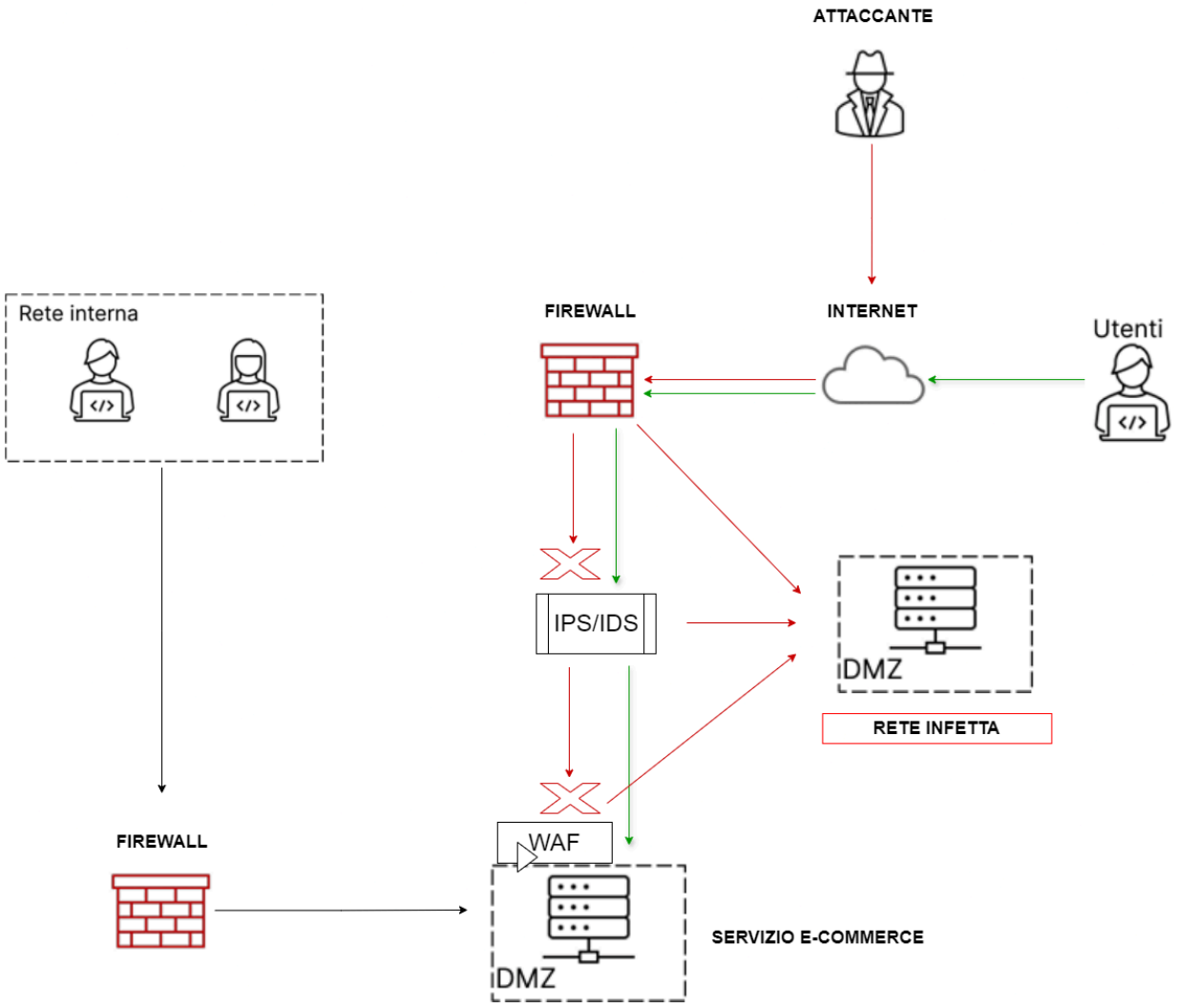
Il firewall, in pratica, se correttamente impostato, smisterà le connessioni in entrata automaticamente verso il server infetto per gli agenti malevoli e verso il server di backup per gli agenti autorizzati.



QUESITO n.4 E SVOLGIMENTO

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

Di seguito, uno schema che riassume la coesistenza delle misure preventive espresse nel quesito n.1 unite alla response del quesito n.3.



QUESITO n.5 E SVOLGIMENTO

Modifica «più aggressiva» dell'infrastruttura (se necessario/ facoltativo magari integrando la soluzione al punto 2).

L'alternativa più aggressiva di risposta a un attacco sarebbe quella di isolare completamente la rete, bloccando qualsiasi tipo di connessione. Scelta altamente invalidante sia per gli utenti che devono acquistare sull'e-commerce che per i dipendenti, potrebbe essere preferibile non applicarla a seconda delle esigenze e della gravità specifiche di quel momento.