Esercizio Finale Modulo 5

In base a quanto richiesto nella traccia, andremo a modificare e mettere in sicurezza l'architettura di rete dell'e-commerce.

Per quanto riguarda le prevenzioni del primo punto, andremo ad applicare le seguenti precauzioni:

- la validazione e la sanificazione dei dati di input dell'utente, ovvero verificare e personalizzare delle regole, come l'eliminazione di certi caratteri pericolosi, sfruttabili dagli attaccanti.

- utilizzare solamente query parametrizzate, in modo tale da evitare di concatenare query SQL dinamiche ai dati di input belle query. Separare i comandi SQL dalla parte dei dati permette di prevenire gli attacchi di SQL Injection.

- escape dei caratteri speciali, ovvero assicurarsi di convertire i caratteri speciali in caratteri sicuri quando vengono visualizzati o inseriti nel codice HTML, questo per proteggersi dal XSS.

- è importante anche la validazione lato server, non solo client(ad esempio Javascript), soprattutto per bloccare gli attacchi che bypassano il lato cliente.

- aggiornamento dei vari software applicativi utilizzati.

- filtraggio degli input, ovvero implementare un filto per bloccare determinati caratteri sfruttabili dagli attaccanti.

- implementare un sistema di monitoraggio che rilevi e registri gli eventi di sicurezza, come tentativi di attacco o comportamenti sospetti. Il logging invece può essere utilizzato per analizzare gli attacchi e intraprendere azioni correttive.

Pere quanto riguarda il punto 2, il danno economico subito dall'azienda a causa dell'attacco DDoS ammonta a 15000 euro. Mentre le azioni di prevenzione e mitigazione che possiamo adoperare sono le seguenti:

- configurare un Firewall di rete con delle regole di filtraggio del traffico indesiderato. Si possono usare Firewall basati su indirizzi IP, regole o firme per bloccare gli IP degli attaccanti.

- giocare sul limite di richieste che possono essere ricevute da un determinato indirizzo IP oppure il traffico di una sessione in un dato intervallo di tempo.

- il load balancing, implementare un sistema di bilanciamento del carico per distribuire il traffico tra più server, in modo da prevenire il sovraccarico di un determinato server.

- un continuo monitoraggio del traffico tramite strumenti appositi.

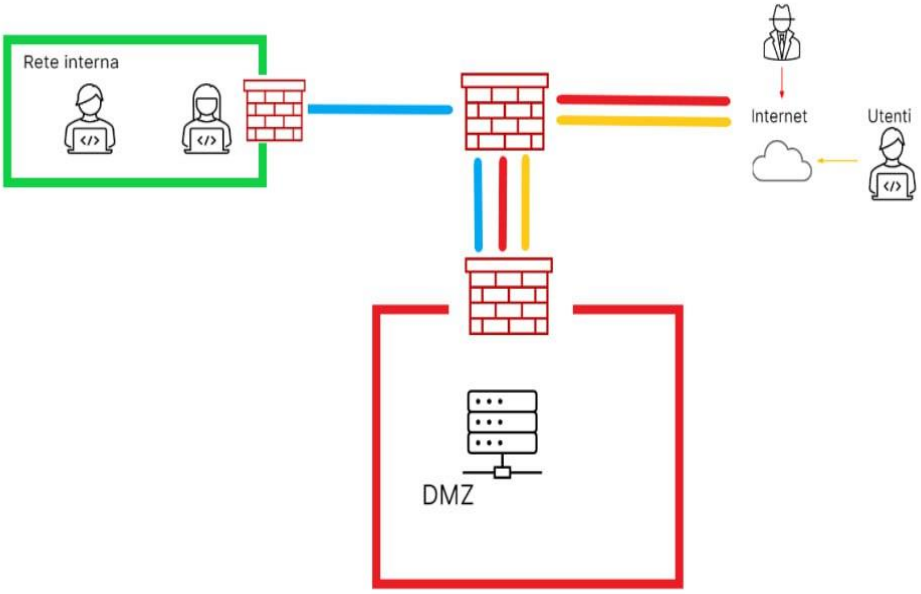
- implementare filtri delle richieste per bloccare e rilevare le richieste sospette che potrebbero essere associate ad attacchi DDoS.

- utilizzare specifici servizi anti-DDos.

- effettuare test di sicurezza specifici regolarmente.

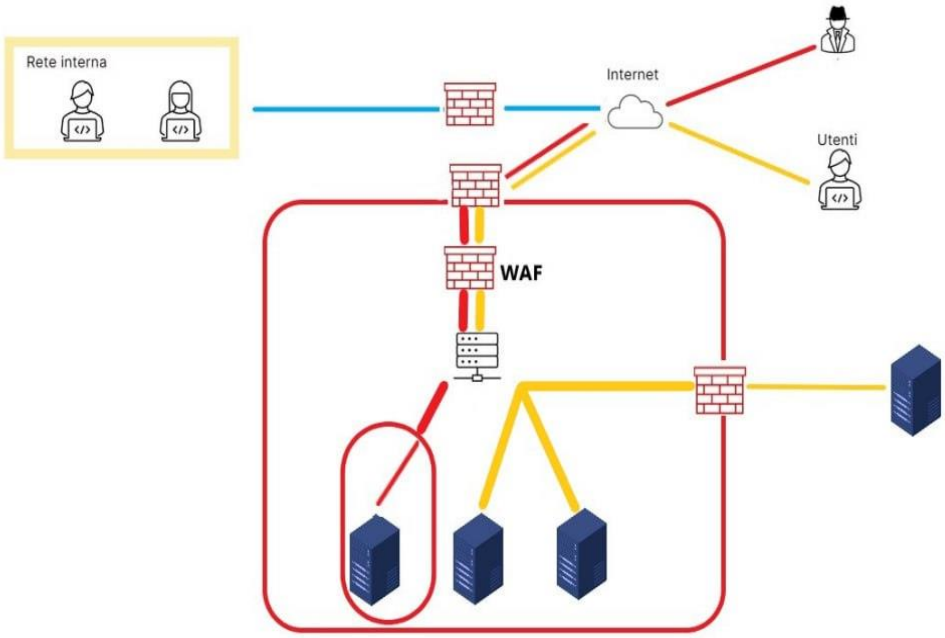
- stilare un piano di azione in risposta ad un eventuale attacco di DDoS.

Per quanto riguarda il punto 3, ho deciso di unirlo al punto 4, e applicare le misure necessarie al network in difesa di un eventuale attacco malware, utilizzando le seguenti modifiche:



Sostanzialmente oltre ad implementare le regole necessarie a mitigare la minaccia, ho aggiunto un WAF al DMZ dell'e-commerce per ulteriore protezione e filtraggio del traffico, e un Next-Generation Firewall a perimetro della rete interna, per garantire una difesa serrata.

Per quanto riguarda il punto 5, ho fatto un lavoro più complesso, andando a togliere la connessione della DMZ alla rete interna, creando di fatto due reti separate collegate direttamente a Internet. In questo caso il Firewall a difesa della rete interna è regolato in modo apposito per garantire una difesa totale. Per la DMZ invece ho applicato un Firewall a monitoraggio del traffico di rete che arriva direttamente dall'Internet, il quale funge da difesa perimetrale dell'intera rete, e in più un WAF all'interno a protezione diretta della DMZ.


Rete interna
Internet
Utenti
WAF