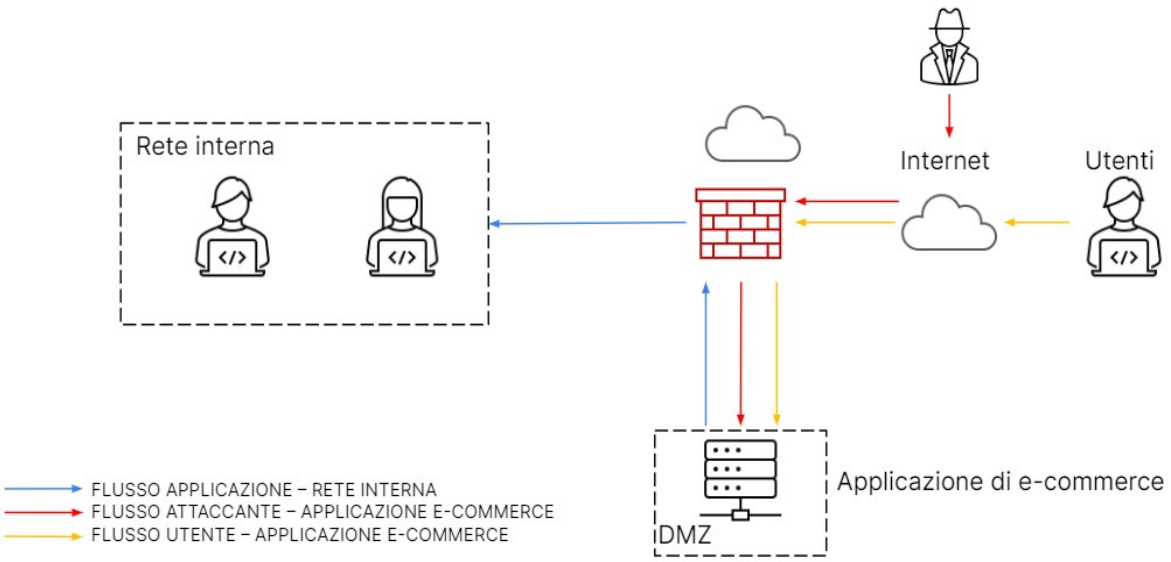
M5 D8

PROGETTO

Questa è l' architettura di rete che si esamina, l' applicazione e-commerce deve essere disponibile per gli utenti tramite Internet per effettuare acquisti sulla piattaforma.

Rete interna raggiungibile dalla DMZ per via delle policy sul firewall , quindi se il server DMZ fosse compromesso allora un attaccante potrebbe raggiungere la rete interna.



1) **Azioni preventive:**

Quali azioni si potrebbero implementare per difendere l' app Web da attacchi di tipo SQLi o XSS da parte di un utente malintenzionato?

Alcune azioni prioritarie possono essere: la sanificazione e validazione dei dati di input dell' utente, specialmente cercando anche di filtrarli per evitare l' inserimento e il successivo utilizzo di script malevoli nell' eventualità di un attacco XSS (Cross-Site Scripting). Questo attacco permette di sottrarre dati sensibili, manipolando il contenuto della pagina vittima, reindirizzando l' utente verso siti ingannevoli oppure installando una backdoor tramite script.

Utilizzo di query SQL parametrizzate in modo tale da evitare di concatenare query SQL dinamiche ai dati input delle query. Se si separano i comandi SQL dalla parte dei dati si può cercare di prevenire eventuali attacchi SQL injection.
Si tratta di inserire codice SQL malevolo all' interno di una query eseguita dal database; consentendo all' attaccante di ottenere accesso a dati sensibili con possibilità di assumerne il pieno controllo.

Assicurarsi di convertire caratteri speciali in caratteri sicuri, una volta visualizzati o inseriti nel codice HTML, per proteggersi specialmente dagli XSS.

Un'altra prevenzione verso gli SQLi si ha con l' utilizzo dell' ORM (Object-Relational Mapping). Consente di mappare le entità e relazionare il database su oggetti propri del linguaggio utilizzato, evitandoci la scrittura di complesse queries SQL.

Per bloccare attacchi che bypassano il lato client, utile la sanificazione e validazione lato server.

Mantenere aggiornati i vari software applicativi utilizzati.

Implementazione di un WAF (Web Application Firewall) prima del server.
Obiettivo è aumentare la protezione tra app web e utenti, filtrando il traffico HTTP/HTTPS e analizzando le varie richieste.
Il WAF identifica e blocca le richieste ritenute dannose o non sicure che potrebbero rappresentare una minaccia, filtra le richieste, rileva eventuali vulnerabilità, protegge eventuali attacchi sia a livello applicativo sia DdoS e monitora e registra il traffico.

Anche il logging potrebbe essere utile per analizzare attacchi di malintenzionati e intraprendere azioni correttive.

2) **Impatti sul business**

L'app Web subisce un attacco di tipo DdoS dall' esterno che rende l' app 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 1500€ sulla piattaforma e-commerce. Fare eventuali valutazioni di azioni preventive che si possono applicare per questa problematica.

Tenendo conto 1500€ /min se ipotizzassimo un guasto lungo 10 minuti, il danno sarebbe 15000€ .

Le azioni di prevenzione e mitigazione che possiamo apportare sono: continuo monitoraggio del traffico, configurare un Firewall di rete con delle regole di filtraggio del traffico indesiderato (utilizzo alternativo di Firewall basati su indirizzi IP, regole o firme per bloccare direttamente IP degli attaccanti).

Si possono inserire limiti sulle richieste ricevute da un determinato IP o bloccare il traffico di una sessione in un dato periodo di tempo, implementare filtri delle richieste per bloccare e rilevare richieste sospette che potrebbero essere associate ad attacchi DDoS.

Altre azioni come implementare un sistema di bilanciamento del carico (load balancing) per distribuire i traffico tra più server, per poter prevenire un eventuale sovraccarico, effettuare test di sicurezza specifici regolarmente, utilizzare specifici servizi anti-DDoS o stilare un piano di azione in caso di eventuale attacco DDoS.

3) **Response**

L'app Web viene infetta da un malware. La priorità è che il malware non si propaghi sulla rete, mentre non si è interessati a rimuovere l' accesso da parte dell' attaccante alla macchina infettata. Proporre una soluzione possibile.

In caso di attacco malware, sicuramente agire isolando la macchina infetta.

Importante limitare l' accesso alla rete interna per prevenire la propagazione del malware alle restanti macchine collegate o dispositivi vari.

Quindi non si ha ancora la necessità di rimuovere l' attaccante dalla rete in quanto si potrebbe studiare il tipo di attacco per prevenire eventuali minacce future; si può limitare l' accesso alla sola DMZ.

Isolata la macchina vittima si può analizzare il malware per capirne il comportamento e i danni provocati all' infrastruttura di rete. Nel caso si ripeta uno scenario simile si è preparati su come rispondere alla minaccia e prendere determinate decisioni.

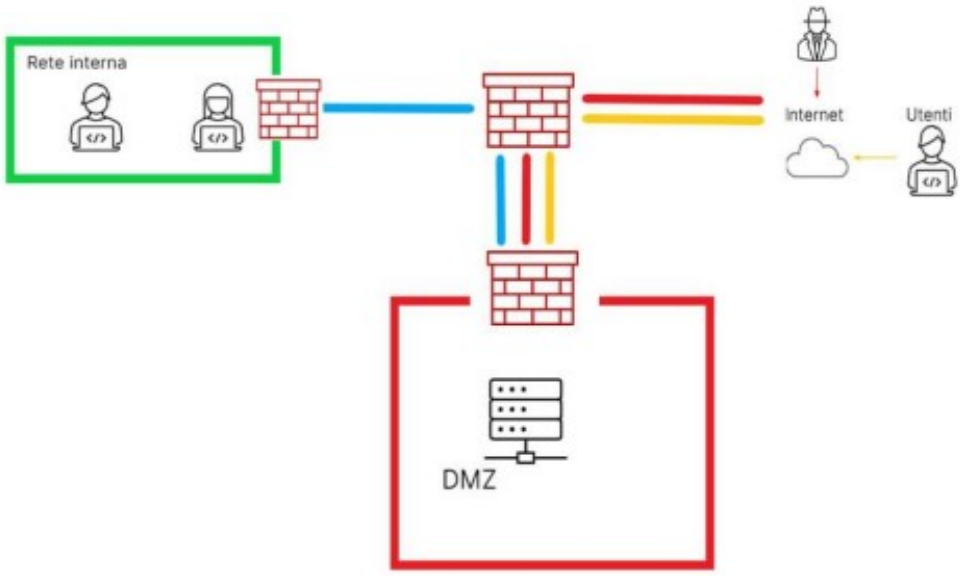
Si può procedere con la rimozione del malware ed effettuare le necessarie pratiche di pulizia e ripristino.

4) **Soluzione completa**

Unire i disegni o spiegazioni dell' azione preventiva e della response (soluzioni punto 1 e 3).

Le azioni preventive sommate e rese complementari sono l' implementazione delle regole necessarie per mitigare la minaccia.

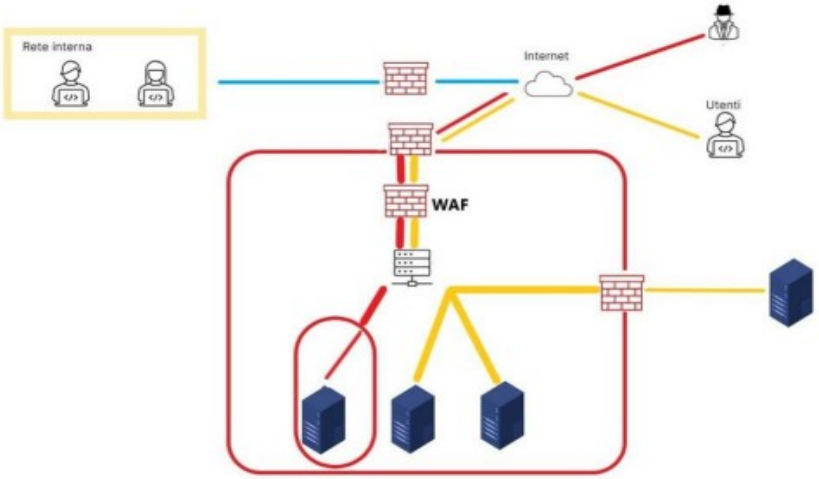
E' presente un WAF in aggiunta al DMZ per un' ulteriore protezione e filtraggio del traffico e in aggiunta un Next-Generation Firewall situato a perimetro della rete interna per poter garantire una protezione ancora più elevata e una difesa maggiore.



5) **Modifica più aggressiva dell' infrastruttura**

Se necessario o facoltativo provare ad integrare questa soluzione con il punto 2.

Le azioni preventive e correttive relativa a questa modalità più aggressiva dell' infrastruttura è più complessa. Riprendendo il punto 2 dove l'app Web subisce un attacco di tipo DdoS dall' esterno e l' app non è raggiungibile per 10 minuti.



In questo caso si elimina la connessione della DMZ dalla rete interna, creando due reti separate collegate direttamente a Internet, il Firewall a difesa della rete interna è regolato in modo apposito per garantire una difesa massima.

Per la DMZ è stato applicato un Firewall a monitoraggio del traffico di rete che arriva direttamente da Internet, il quale si comporta come una difesa perimetrale dell' intera rete e in più presente un WAF all' interno a protezione diretta della DMZ.