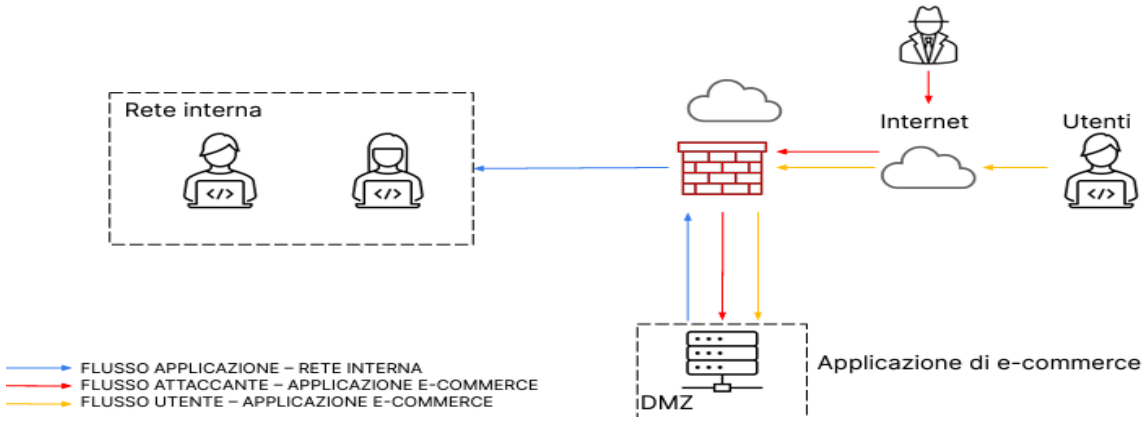
PROGETTO MODULO 5

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.



Traccia: Con riferimento alla figura, 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.

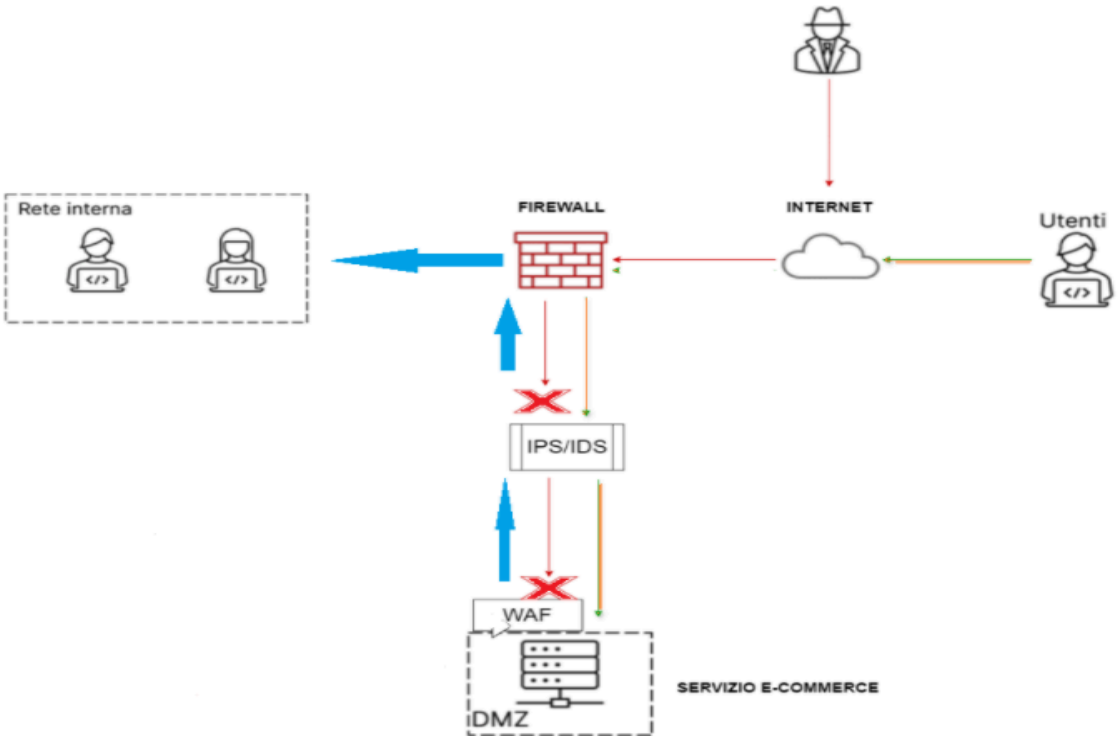
2. Impatti sul business: l'applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione non raggiungibile per 10 minuti. Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media ogni minuto gli utenti spendono 1.500 € sulla piattaforma di e-commerce. 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 vostra rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura 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 integrando la soluzione al punto 2)

1. Un'azione preventiva per proteggere la nostra applicazione di e-commerce potrebbe essere il Web Application Firewall (WAF) che consente di proteggere le applicazioni Web da attacchi dannosi e traffico Internet indesiderato, inclusi bot, injection e (DoS) a livello di applicazione. WAF consente di definire e gestire le regole per evitare minacce a Internet, tra cui indirizzi IP, intestazioni HTTP, corpo HTTP, scripting tra siti (XSS), inserimento SQL e altre vulnerabilità definite da OWASP. Il WAF può essere configurato per registrare e monitorare tutti i tentativi di attacco SQLi e XSS. Questi log possono essere utilizzati per analizzare i modelli di attacco, identificare le vulnerabilità dell'applicazione e adattare le regole del WAF di conseguenza. Oltre al WAF potremmo andare ad inserire un sistema di monitoraggio IDS/IPS per rilevare minacce e nel caso di un sistema IPS impedire o mitigare gli attacchi prima che possano causare danni alla rete e al nostro servizio.



Nel grafico sopra possiamo vedere come i sistemi di prevenzione WAF e IPS/IDS si interpongono tra l'applicazione e l'attaccante così da impedirgli l'accesso.

2. **Impatti sul business:**

Per calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio per 10 minuti a causa di un attacco DDoS, possiamo utilizzare la seguente formula:

Impatto sul business = (Durata dell'interruzione) x (Perdita di guadagno per minuto)

Dove:

- Durata dell'interruzione è 10 minuti
- Perdita di guadagno per minuto è 1.500 €

Quindi:

Impatto sul business = 10 minuti x 1.500 €/minuto = 15.000 €

Per ridurre l’impatto sul business potremmo attuare le seguenti misure preventive:

- **Distribuire una rete di server e bilanciare il carico**: Distribuire l'applicazione su più server e utilizzare il bilanciamento del carico per garantire la continuità del servizio anche in caso di attacco a uno dei server.
- **Implementare una Content Delivery Network (CDN)**: Le CDN distribuiscono il contenuto su server geograficamente distribuiti, riducendo la latenza e distribuendo il carico di lavoro per filtrare il traffico dannoso durante gli attacchi DDoS.
- **Monitoraggio continuo e piani di risposta**: Monitorare costantemente il traffico di rete e avere piani di risposta agli incidenti ben definiti, inclusa la collaborazione con esperti di sicurezza informatica per risolvere rapidamente gli attacchi e ripristinare il servizio.

Il costo dell'implementazione delle misure di prevenzione contro gli attacchi DDoS può variare in base alle dimensioni dell'azienda. Tuttavia, considerando l'impatto stimato di 15.000 euro per un singolo attacco DDoS di 10 minuti, vale la pena valutare l'investimento in queste misure preventive.

Se l'azienda prevede di subire attacchi DDoS in futuro, l'implementazione delle misure preventive potrebbe essere vantaggiosa sia finanziariamente che in termini di reputazione aziendale e continuità operativa. Senza queste misure, si rischia non solo perdite finanziarie durante gli attacchi, ma anche danni alla reputazione e possibile perdita di clienti a lungo termine dovuti all'inaccessibilità del servizio.

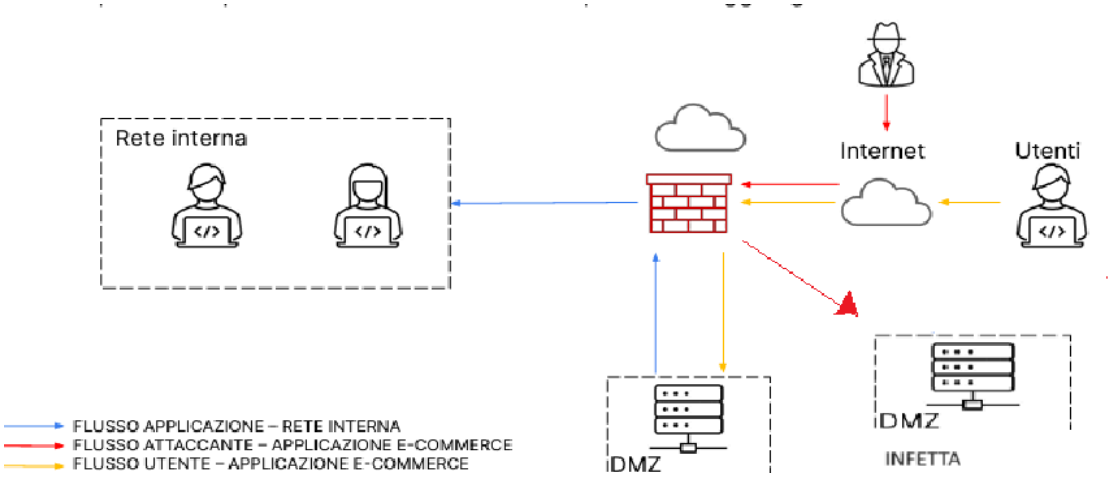
Inoltre, è importante considerare che l'impatto degli attacchi DDoS potrebbe essere più grave in futuro, con potenziali perdite finanziarie ancora più elevate. Pertanto, investire in misure preventive può essere una decisione strategica a lungo termine per proteggere l'azienda e garantire la continuità delle operazioni.

3. **RESPONSE:**

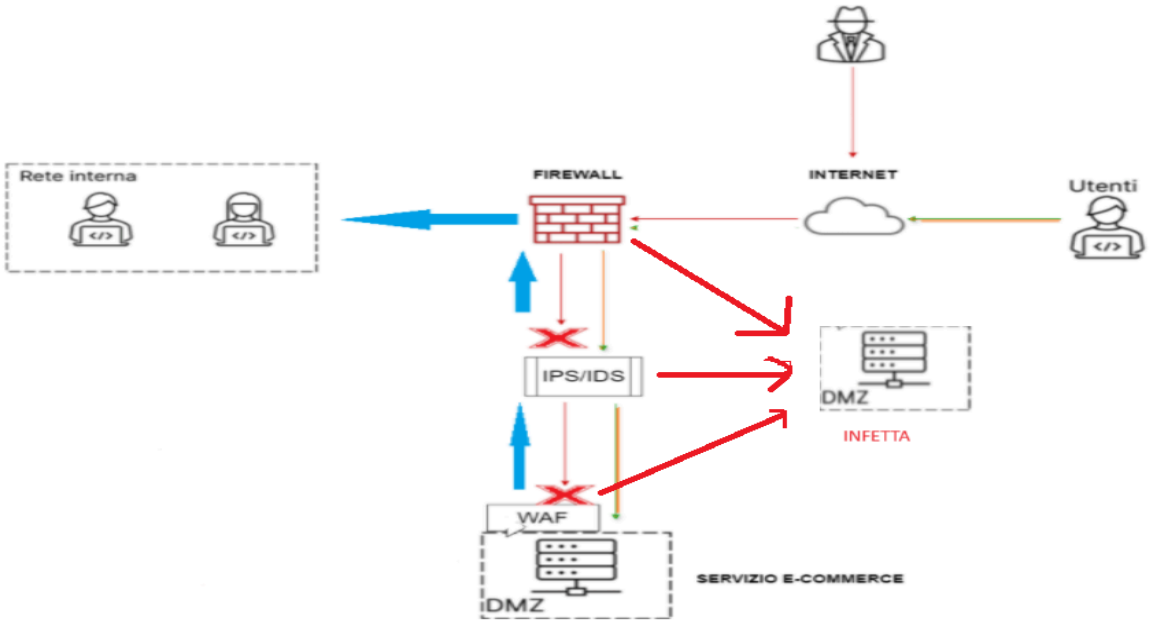
L'applicazione web è stata infettata dal malware. L'attaccante è riuscito ad infettare con un malware la nostra app di e-commerce.

Ipotizziamo di avere una seconda DMZ per garantire l'utilizzo del servizio. Come azione primaria andremo ad isolare il sistema DMZ infetto così da instradare il traffico dell'attaccante limitando ulteriori danni.

Questa azione ci permette di proteggere la rete interna e mantenere i servizi attivi per gli utenti mentre possiamo mantenere l'accesso dell'attaccante alla macchina infetta per ulteriori analisi.



4. Soluzione completa Di seguito un grafico con le azioni preventive ipotizzate nel punto 1 e 3.



5. Modifica aggressiva:

Isolamento: una soluzione per rispondere all’attacco potrebbe essere quella di isolare completamente il sistema infetto bloccando qualsiasi tipo di connessione.

Blocco totale del traffico: Bloccare immediatamente ogni tipo di traffico in entrata e in uscita dalla macchina infetta per prevenire qualsiasi comunicazione con l'esterno.

Analisi forense: Avviare un'analisi approfondita per identificare l'origine e il comportamento del malware, acquisendo informazioni utili per rafforzare la sicurezza dell'infrastruttura.

Riorganizzazione della sicurezza: Rivedere e rafforzare l'intera strategia di sicurezza, implementando controlli più rigorosi.

Formazione del personale: Fornire una formazione intensiva al personale per aumentare la consapevolezza sulla sicurezza informatica e prevenire futuri attacchi.

Penetration test: Condurre test regolari di penetrazione per identificare vulnerabilità nell'infrastruttura e rafforzare le difese contro potenziali minacce.

Attuare queste misure drastiche non è sempre consigliato perchè il blocco totale delle connessioni e il blocco del traffico potrebbe causare disservizi sia per gli utenti che per i dipendenti e quindi potrebbe portare ad una notevole perdita finanziaria e di conseguenza ad una perdita di reputazione.

Inoltre applicare queste misure implica costi aggiuntivi in termini di risorse umane e finanziarie per una analisi approfondita.

Pertanto, è fondamentale bilanciare l'adozione di misure aggressive con la comprensione delle potenziali conseguenze negative e valutare attentamente i rischi e i benefici di ciascuna azione.

Leonardo Margheri