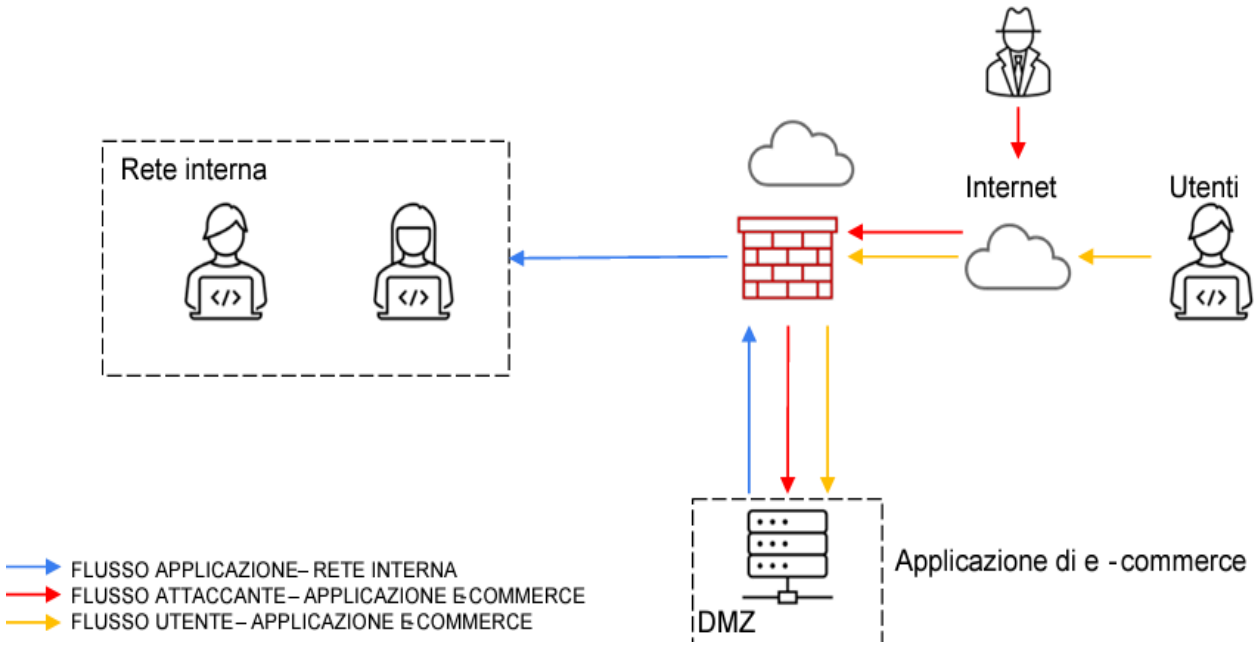
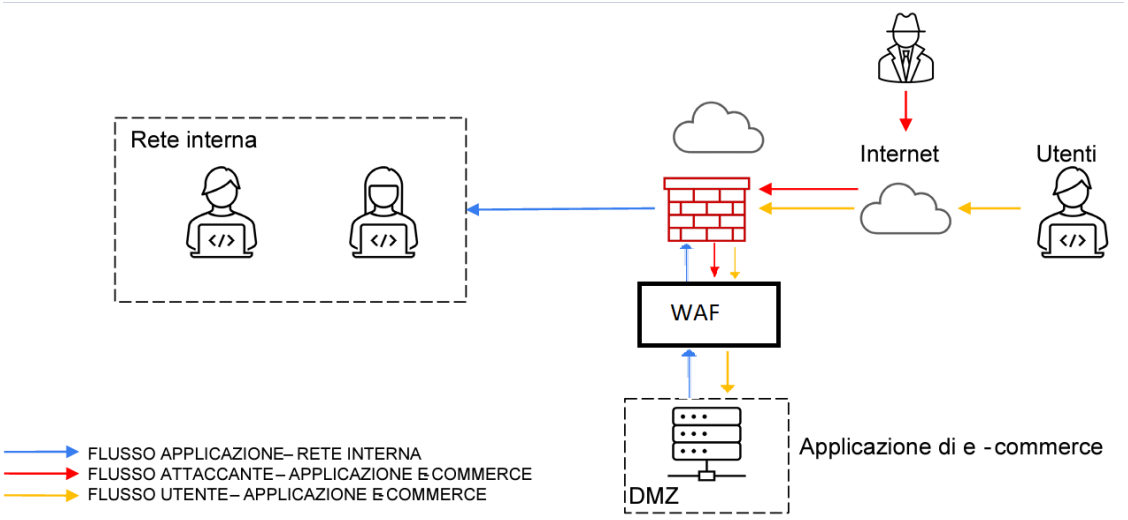
S9/L5

Traccia:
Con riferimento alla figura in slide 2, 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 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: integrando eventuali altri elementi di sicurezza (se necessario/facoltativo magari integrando la soluzione al punto 2.)



1-AZIONI PREVENTIVE:
Il primo quesito ci chiede di individuare delle azioni preventive per difendere l'applicazione di e-commerce da attacchi di tipo SQLi oppure XSS.
Tra le azioni preventive che possiamo integrare vi è l'inserimento di un WAF (Web Application Firewall). Inserire un WAF tra il firewall e la DMZ dove vi è l'applicazione web, consente di aggiungere uno strato di sicurezza progettato per proteggere le applicazioni web dalle minacce online.
Essenzialmente, un WAF agisce come uno scudo protettivo tra l'applicazione web e Internet, filtrando il traffico dannoso e applicando politiche di sicurezza per prevenire attacchi come SQL Injection e XSS, in quanto un WAF analizza le richieste HTTP in ingresso per individuare degli script dannosi o sequenze tipiche di tentativi di iniezione SQL bloccando le richieste sospette.



2-IMPATTO 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.

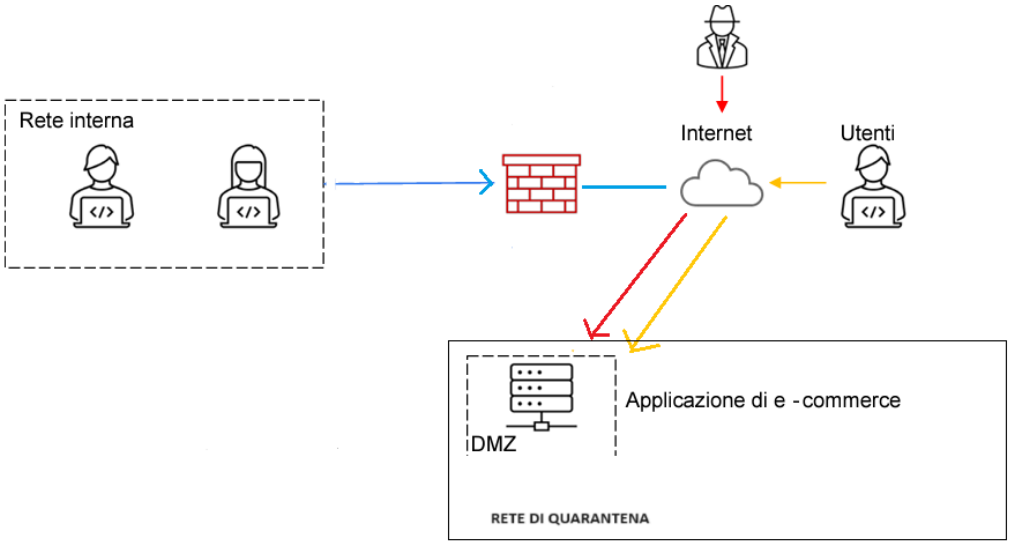
Dato che l'attacco ha reso l'applicazione non raggiungibile per 10 minuti e che gli utenti spendono in media 1.500 € al minuto, possiamo calcolare l'impatto finanziario come segue:

Impatto finanziario = 10 minuti * 1.500 €/minuto = 15.000 €

Quindi, l'impatto finanziario dovuto alla non raggiungibilità del servizio è di 15.000 €.

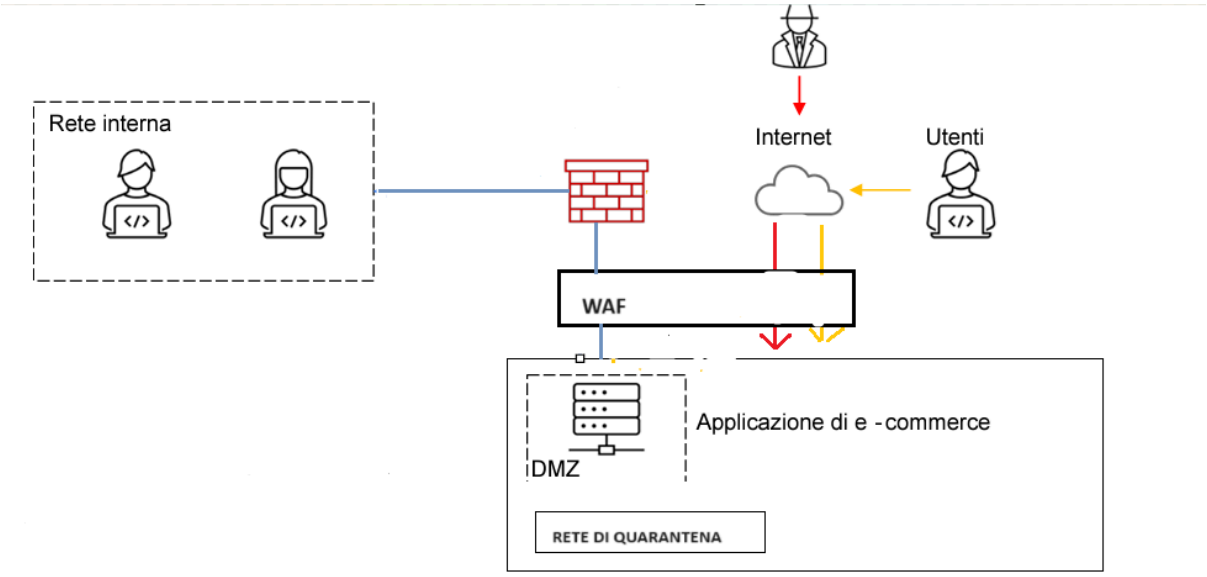
Per mitigare gli effetti di futuri attacchi DDoS, possono essere adottate diverse azioni preventive. Come per esempio l'implementazione di un buon Business Continuity Plan (BCP), il quale permetterebbe ad un servizio di continuare ad operare anche in situazioni critiche, (esempio di attacco DDoS), danni accidentali o calamità naturali. Bisogna dunque identificare i fattori di rischio e calcolarne l'impatto che avrebbe sull'azienda. Per ridurne l'impatto inoltre, è molto utile effettuare un full back-up. Se l'attacco DDoS interrompe il normale flusso di operazioni, un backup completo consente di ripristinare rapidamente i dati e le configurazioni dell'applicazione allo stato precedente all'attacco e può consentire alla piattaforma di tornare online più velocemente, riducendo l'impatto sulla clientela e sulle entrate. Tuttavia, è fondamentale assicurarsi che i backup siano aggiornati regolarmente e che siano conservati in un luogo sicuro e isolato dagli attacchi, in modo che siano disponibili quando necessario.

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 .

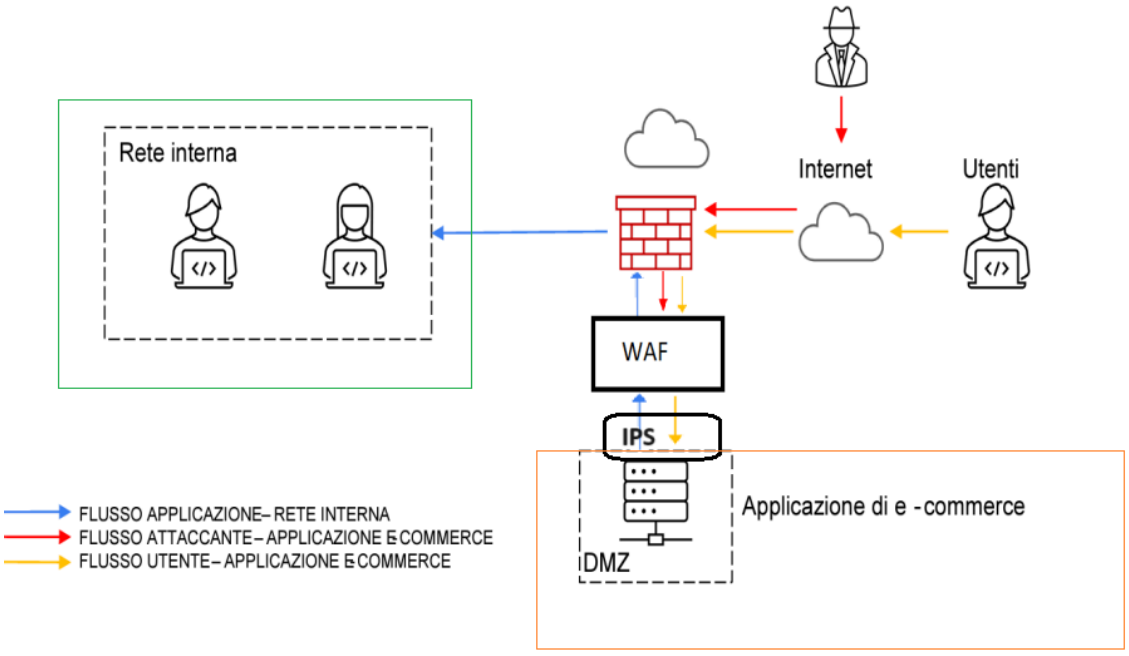


In questo caso, l'attaccante ha infettato l'applicazione dell'e-commerce attraverso un malware. Il nostro scopo è quello di contenere il malware e non farlo propagare nella rete interna,così che tenendolo separato non sarà in grado di riprodursi. Creiamo dunque una rete di quarantena, attraverso la tecnica dell'isolamento.
L'isolamento consiste nella completa disconnessione del sistema infetto dalla rete, in modo tale che l'attaccante non abbia accesso alla rete interna. In questo caso però, non essendo interessati a rimuovere l'attaccante dalla macchina infetta, notiamo che ha ancora accesso al sistema tramite internet.

4-SOLUZIONE COMPLETA:



5-Modifica «più aggressiva» dell'infrastruttura: integrando eventuali altri elementi di sicurezza



Come possiamo vedere dalla figura, abbiamo aggiunto un sistema di Prevenzione delle Intrusioni (IPS) direttamente di fronte al server dell'applicazione in modo tale da fornire una difesa proattiva e in tempo reale contro una vasta gamma di minacce, contribuendo a garantire la sicurezza e l'integrità dei dati e delle risorse informatiche

di un'organizzazione. Questo grazie alla sua attività di monitoraggio del traffico in entrata e in uscita.
Inoltre, per migliorare la gestione del sistema abbiamo segmentato la rete, grazie al subnetting, il quale consente di creare segmenti di rete separati e isolati, migliorando il controllo e la sicurezza della rete; è infatti possibile applicare politiche di sicurezza diverse a ciascuna sotto-rete e limitare l'accesso a risorse specifiche in base alle esigenze di sicurezza dell'organizzazione.

BONUS:
Analizzare le seguenti segnalazioni caricate su anyrune fare un piccolo report di ciò che si scopre relativo alla segnalazione dell'eventuale attacco spiegando ad utenti e dirigenti la tipologia di attacco e come evitare questi attacchi in futuro:

1) https://app.any.run/tasks/8e6ad6d9-4d54-48e8-ad95-bfb67d47f1d7/

Analizzando il contenuto vediamo "PERFORMANCE_BOOSTER_v3.6.exe", il quale sembra essere il nome di un file eseguibile, che potrebbe essere un software progettato per migliorare le prestazioni del computer. Tuttavia, possiamo vedere che il termine "booster" potrebbe anche essere utilizzato per indicare un software potenzialmente dannoso, perciò prima di eseguire questo file sui computer, è importante verificare che la fonte sia sicura e attendibile.

Infatti, vediamo in realtà che può andare a modificare le impostazioni di sicurezza di PowerShell per eseguire dei comandi senza restrizioni e può leggere informazioni sensibili dal registro di sistema. Per cui in sintesi può danneggiare il sistema attraverso comandi dannosi, rubare informazioni e consentire l'accesso non autorizzato al computer.