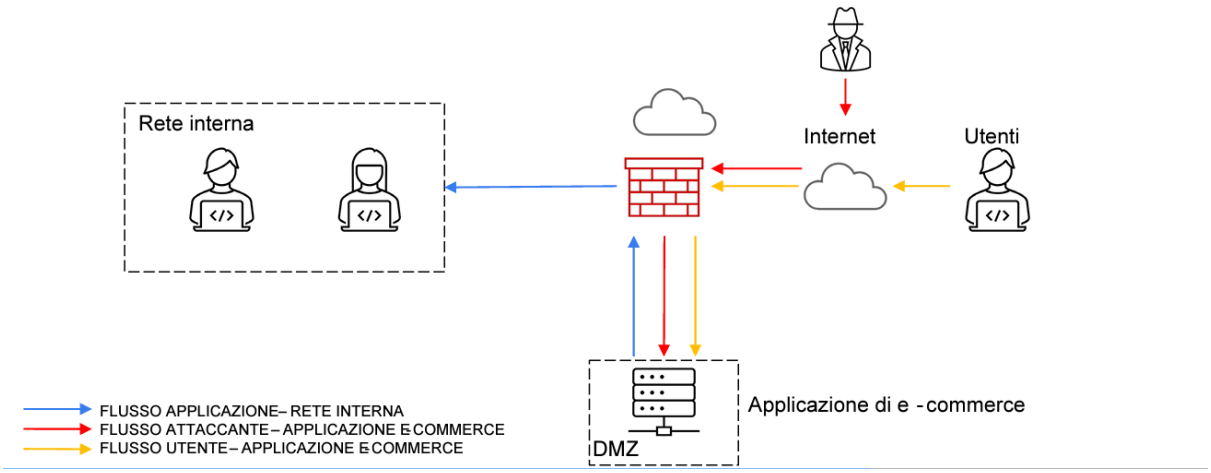
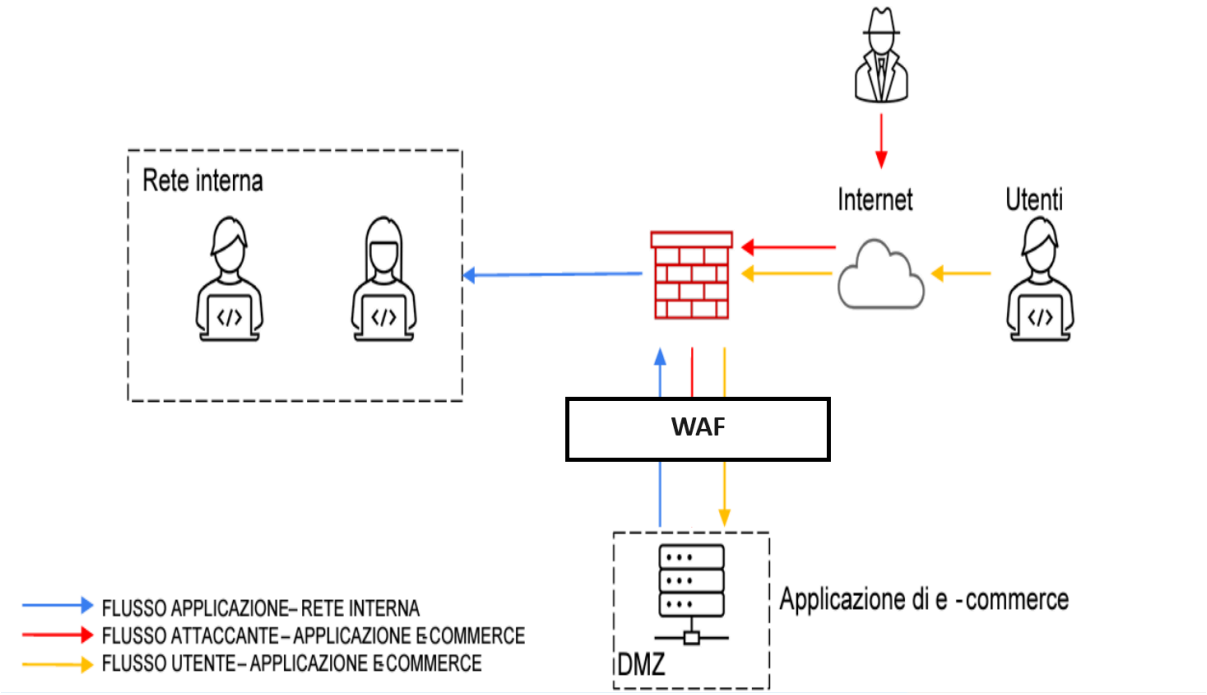
PROGETTO SETTIMANA 9

Nell’esercizio di oggi abbiamo la situazione sottostante di partenza, da questa situazione ci viene richiesto di effettuare varie modifiche e scelte per migliorare la sicurezza della rete.



1)AZIONI PREVENTIVE

Ci vengono richieste quali azioni preventive si potrebbero implementare per difendere l’applicazione WEB da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato e modificare il disegno di partenza. Per prevenire attacchi di questo genere possiamo utilizzare un web application firewall (WAF), è un tipo di firewall progettato specificamente per proteggere le applicazioni web da attacchi informatici. Funziona analizzando il traffico HTTP tra un browser web e l'applicazione web e filtrando o bloccando il traffico che potrebbe essere dannoso o non autorizzato. In sostanza, il WAF aiuta a proteggere le applicazioni web da vulnerabilità e attacchi come SQL injection, cross-site scripting (XSS) e altri. Come vediamo nell’immagine il criminale arriva al WAF ma non riesce ad arrivare all’applicazione e-commerce.

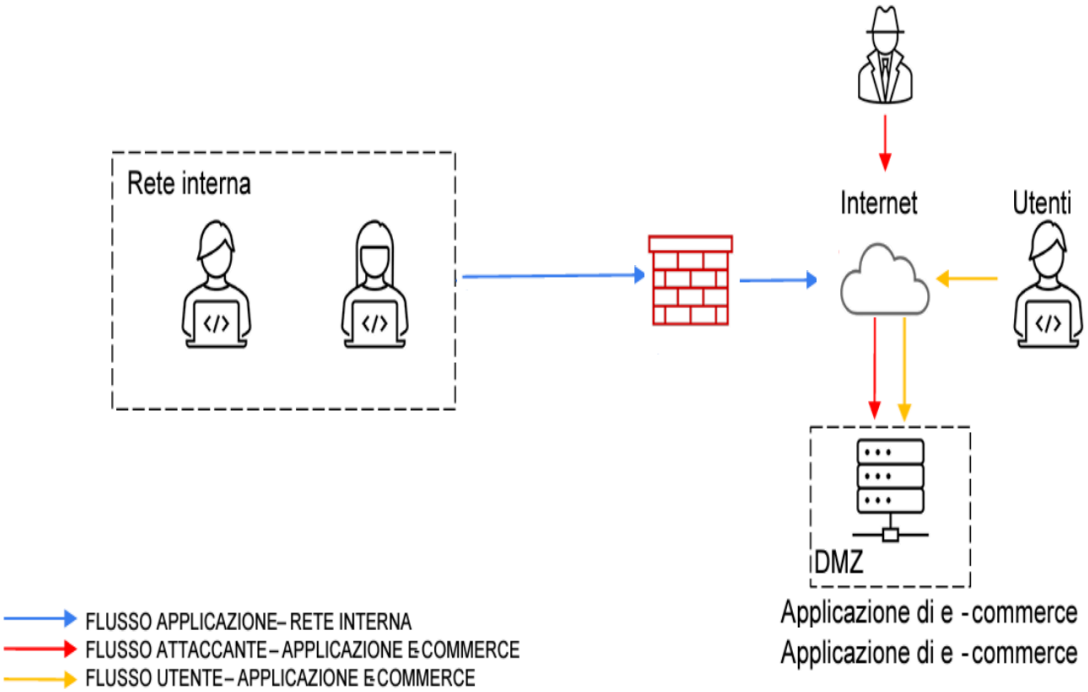


2)IMPATTI SUL BUSINESS

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.
Iniziamo con il calcolo della perdita dei 10 minuti in cui il server è stato non raggiungibile, quindi facciamo 1.500 (euro persi al minuto) * 10 (minuti in cui il server è stato down) = 15.000. Per andare a rendere nullo l'attacco eseguito dal criminale informatico suggerisco di avere sempre un backup e un server di riserva, così facendo se subiamo un attacco DDoS, possiamo eliminare momentaneamente il server attaccato e utilizzare il server di riserva con il backup per tornare subito online e non perdere gli incassi procurati dalla piattaforma di e-commerce.

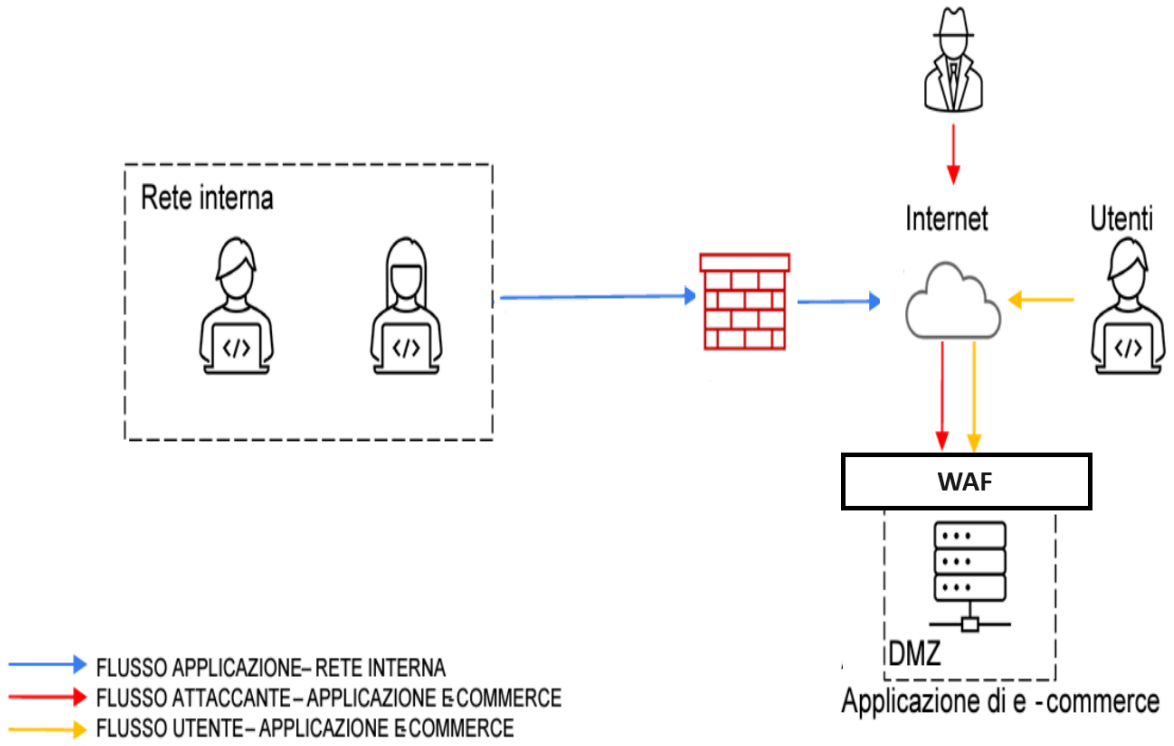
3)RESPONSE

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 .
Per riuscire ad eliminare il contatto con la rete interna da parte del server infetto e lasciare l’accesso all’attaccante utilizziamo l’isolamento. L’isolamento consiste nella completa disconnessione del sistema infetto dalla rete,per restringere ancora maggiormente l'accesso alla rete interna da parte dell'attaccante. Andiamo ad isolare la parte infetta senza rimuoverla per poter studiare il comportamento dell’attaccante, così facendo la parte infetta diventa un vero e proprio honeypot, abbiamo messo in sicurezza la rete poiché il malware non riesce a moltiplicarsi e studiamo anche il suo comportamento.



4)SOLUZIONE COMPLETA

Ora ci viene richiesto di unire il primo disegno con il terzo, quindi notiamo che abbiamo l'applicazione web isolata con a protezione il WAF.



5)MODIFICA DELL'INFRASTRUTTURA

Altri elementi di sicurezza da implementare possono essere ad esempio il backup come abbiamo detto per il punto numero 2. Una buona idea sarebbe quella di avere un monitoraggio avanzato del traffico di rete.
Il monitoraggio avanzato del traffico di rete è un'attività che coinvolge la raccolta, l'analisi e l'interpretazione dei dati relativi al traffico di rete all'interno di un'infrastruttura IT. Le principali attività sono:

Raccolta dei dati: Vengono raccolti dati dettagliati sul traffico di rete da dispositivi come switch, router, firewall e sensori di monitoraggio del traffico.
Analisi dei dati: I dati raccolti vengono analizzati per individuare pattern, anomalie o comportamenti sospetti. Questo può includere l'identificazione di volumi di traffico insoliti, flussi di dati non autorizzati o tentativi di accesso non autorizzati.
Interpretazione dei dati: Gli analisti interpretano i dati per comprendere meglio le tendenze del traffico di rete, individuare potenziali minacce alla sicurezza e valutare le prestazioni della rete.
Identificazione delle minacce: Il monitoraggio avanzato del traffico di rete consente di individuare attività dannose o potenzialmente dannose, come attacchi informatici, malware, tentativi di accesso non autorizzato e altri comportamenti malevoli.
Risposta alle minacce: Una volta individuate le minacce, vengono attivate misure di risposta appropriate, che possono includere l'isolamento di dispositivi compromessi, la mitigazione degli attacchi in corso e l'applicazione di politiche di sicurezza aggiuntive.
Ottimizzazione delle prestazioni: Oltre alla sicurezza, il monitoraggio avanzato del traffico di rete può essere utilizzato per ottimizzare le prestazioni della rete, identificando e risolvendo eventuali congestioni o problemi di larghezza di banda.
In sintesi, il monitoraggio avanzato del traffico di rete è fondamentale per garantire la sicurezza e le prestazioni ottimali delle reti aziendali, consentendo di rilevare e rispondere prontamente alle minacce informatiche e di ottimizzare l'efficienza complessiva della rete.
Quindi possiamo implementare un IPS ed un IDS che eseguono monitoraggio, implementiamo anche software in grado effettuare il monitoraggio come Wireshark.