

Incident Response Progetto S9-L5

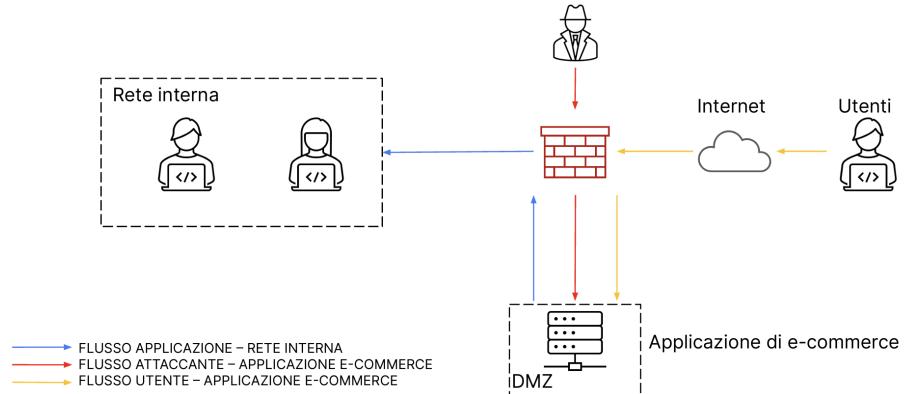
Traccia

- 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.

- 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.

Design di rete fornito

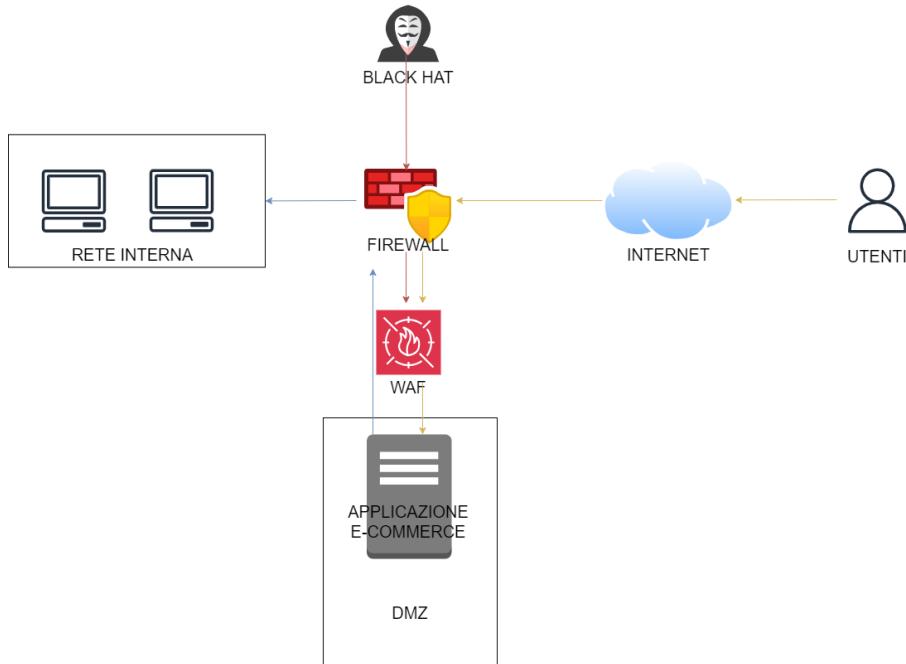


1. Azioni Preventive

Prendendo come caso di studio il design fornитoci, si è in grado di capire di un grande problema, o meglio, una grande mancanza in ambito di prevenzione e sicurezza.

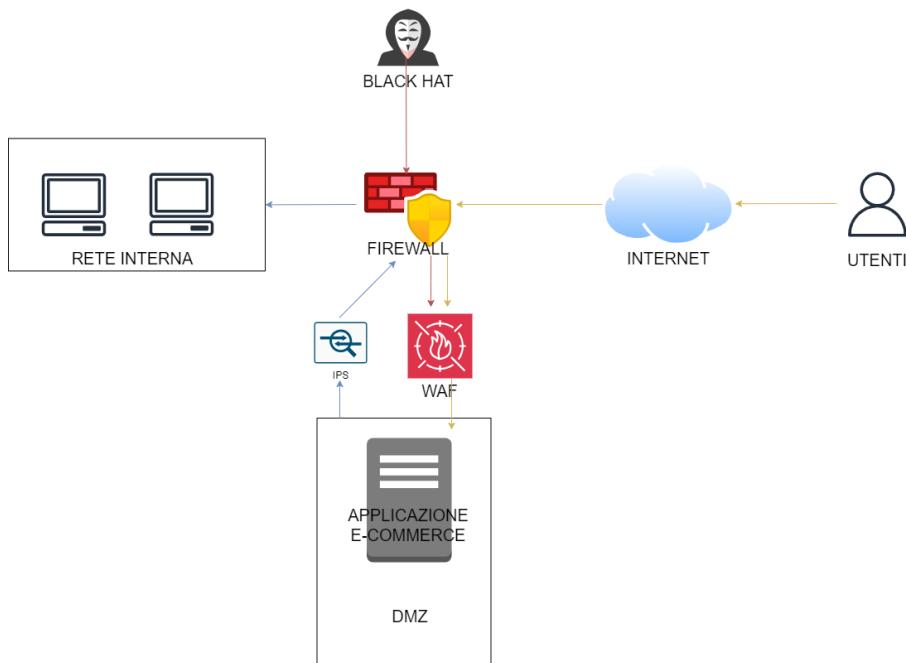
Il problema è risolvibile inserendo correttamente un WAF, in modo che quindi si impedisca ad un attaccante di poter eseguire gli attacchi XSS e SQLi (visti nelle lezioni precedenti).

Il WAF è un firewall adibito specificatamente allo scopo di lavorare al livello di applicazione, analizzando le connessioni HTTP tra le web app e i client. Le regole del WAF sono poste in modo che ogni richiesta di connessione HTTP venga identificata e filtrata, limitando quindi il pericolo di attacchi mirati a vulnerabilità delle applicazioni web, tra cui appunto, i due menzionati sopra.



Implementando il WAF tra la rete interna e rete esterna si andrà a proteggere la zona demilitarizzata DMZ, rendendo molto più difficile il lavoro dell'attaccante nel far eseguire uno script nel sito e allo stesso tempo mantenendo intatti i rapporti con gli utenti legittimi che voglio vistare il sito.

Questo basta per avere la sicurezza che un attaccante non possa entrare? No, la sicurezza al 100% non esiste, ma il WAF offre un elevato tasso di sicurezza. Le probabilità di successo potrebbero essere ulteriormente rafforzate ponendo un IPS tra il server web app e la rete interna.



2. Impatti sul Business

Nel caso posto dall'esercizio, apprendiamo che la web app dell'azienda subisce un attacco DDOS che la rende inagibile per 10 minuti. L'attacco DDOS rende inagibile la web app proprio a causa della sua funzione, ossia un attacco massiccio che sfrutta una BOTNET (centinaia se non migliaia di dispositivi fisici sotto il controllo di uno o più attaccanti) che invia una quantità enorme di input, i quali possono saturare la rete oppure superare la capacità del server e dei suoi processori di elaborare le tantissime richieste.

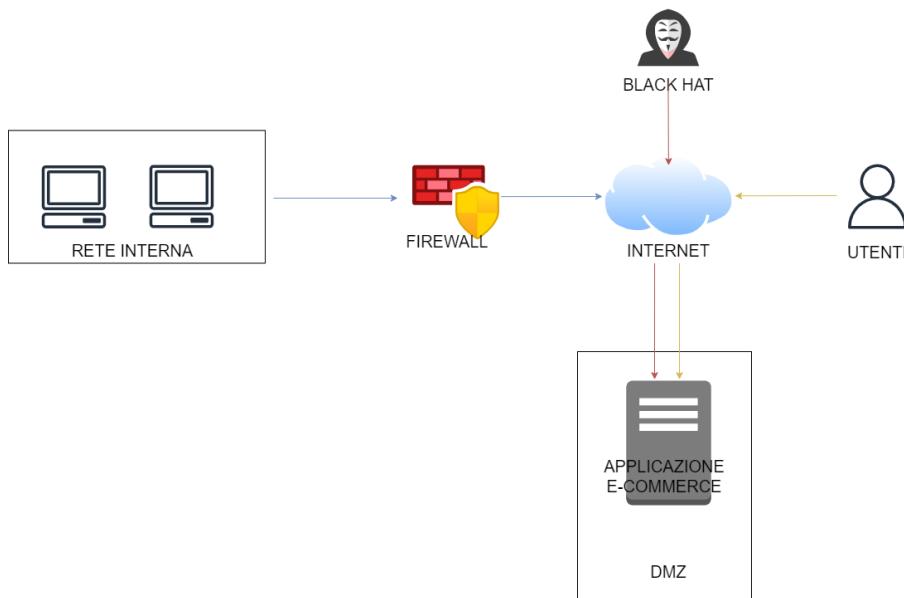
Per calcolare l'impatto sul business basta fare un semplice calcolo, avendo a disposizione il dato di quanto spendono gli utenti in media al minuto.

$$\text{Impatto} = 1500\text{€}/\text{minuto} * 10 \text{ minuti} = 15.000\text{€}$$

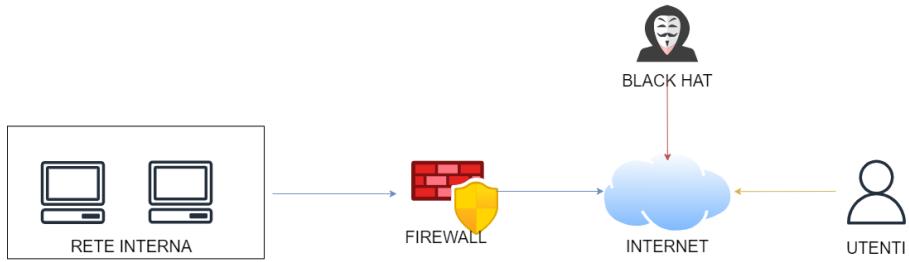
Questa cifra potrebbe avere un impatto basso, medio o alto in base alla grandezza dell'azienda. Se l'azienda in esempio percepisse un guadagno di 500.000 euro al mese, probabilmente questo impatto calcolato sarebbe di bassa entità, al contrario se l'azienda guadagnasse 10.000 euro al mese, l'impatto sul business dato dall'attacco sarebbe devastante e probabilmente rovinerebbe l'azienda.

3. Response

In questo terzo caso, la web app viene infettata da un malware. Per evitare che il malware si possa propagare anche alla rete interna verrà effettuata un'azione di isolamento. L'isolamento consiste nella completa disconnessione del dispositivo infetto dalla rete interna ma senza rimuovere l'accesso ad internet. In questo modo il malware non avrà un mezzo per diffondersi ulteriormente nella rete locale ma manterrà comunque i propri servizi online (questo però ovviamente comporta un rischio per tutti gli utenti che visiteranno il sito e-commerce, che, a scanso di comunicazioni da parte dell'azienda, saranno ignari della presenza del malware e rischieranno quindi di finire vittima).



Nel caso in cui invece, l'azienda si fosse preoccupata di eventuali malware diffusi agli utenti o della continua possibilità del black hat di poter accedere alla web app, il serve di quest'ultimo sarebbe stato completamente rimosso da tutto, rimuovendo i cavi sia per la rete interna sia per la connessione alla rete globale. In questo modo sarebbe impossibile comunicare con il server se non tramite mezzi fisici come una chiavetta USB.



Questi ultimi due casi comunque fanno parte degli scenari più critici, sui quali è richiesta l'attuazione di misure di sicurezza estreme, soprattutto l'ultimo esempio fatto.

In situazioni “meno critiche” si potrebbe pensare di creare una “rete di quarantena”, usando la segmentazione di rete per erigere una rete apposita su cui mettere il dispositivo infetto, così da limitarne le azioni verso la rete locale principale.