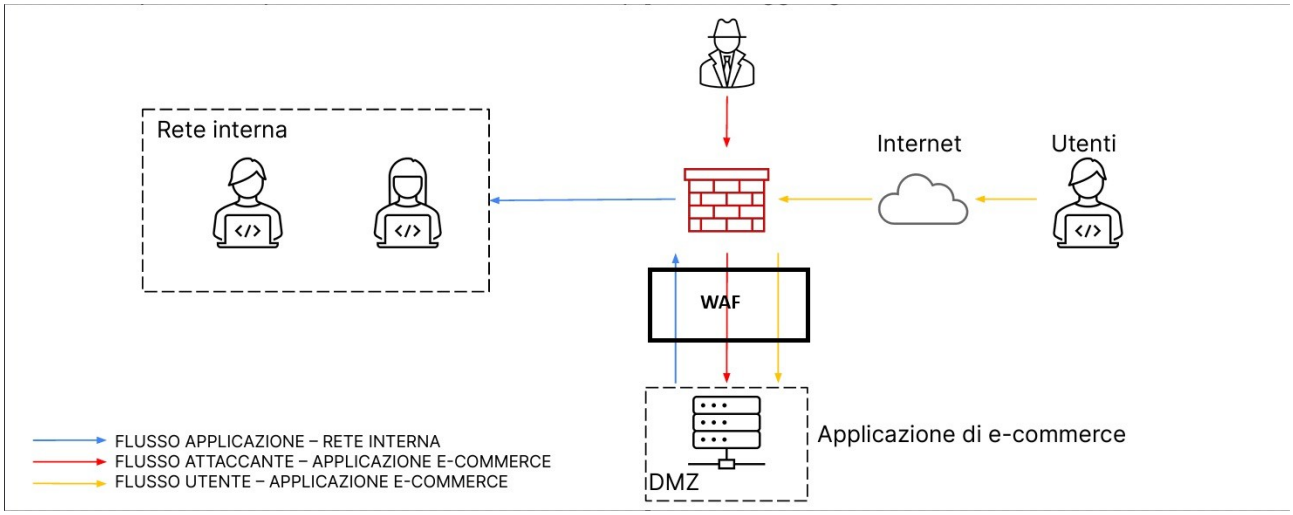
S9L5 Luca Danelli

Domanda 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

Una buona soluzione sarebbe l'introduzione di un WAF a supporto del firewall nella figura proposta, come da immagine sotto:



Essendo l'applicazine di e-commerce presente nella DMZ, il firewall perimetrale installato permetterà le richieste dal e verso il Web Server senza protezione aggiuntiva. Un Web Application Firewall quindi sarebbe la soluzione ideale perché andrebbe a confrontare le richieste da parte degli utenti (ed eventuali attaccanti) con il proprio database, alla ricerca di possibile codice malevolo che potrebbe venire iniettato all'interno delle applicazioni dando vita appunto ad un attacco di tipo SQLi o XSS.

Il WAF può essere un apparato fisico collegato alla rete o anche un modulo logico presente nel Firewall stesso, che andrebbe ad analizzare solo le richieste relative alla DMZ.

Va inoltre ricordato che nonostante il WAF offra un ottimo livello di protezione, è opportuno modificare il codice delle applicazioni WEB in modo che l'input dell'utente risulti sanato, ossia non accetti in input eventuali caratteri che potrebbero essere interpretati come script dai server di Back-End o dal Database SQL

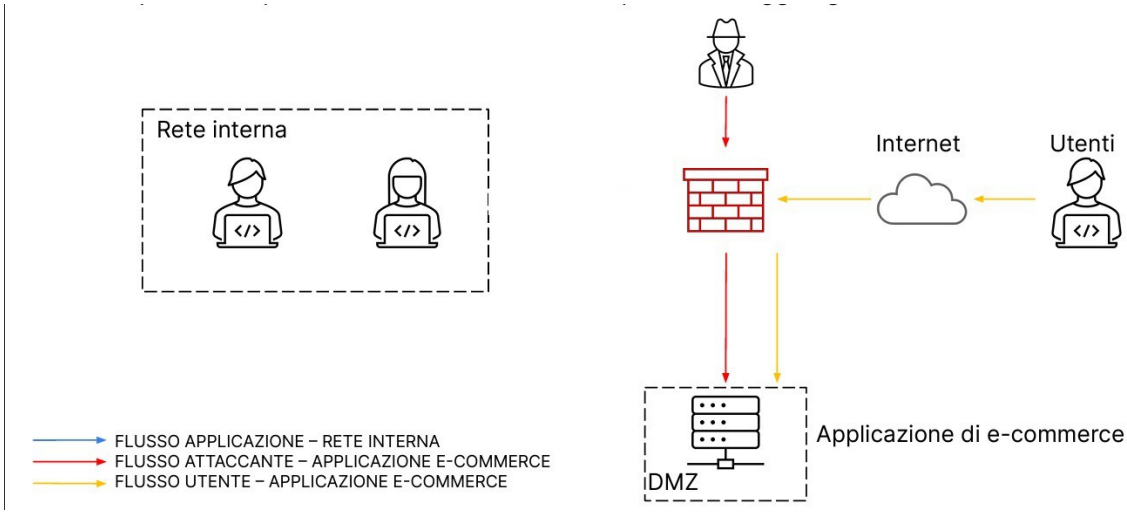
Domanda 2:

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.

Sapendo che l'azienda in questione incassa 1500€ ogni minuto dalla vendita dei propri beni tramite l'applicazione di e-commerce, possiamo quantificare una perdita di 15000€ dovuti all'assenza di servizio per 10 minuti causata dall'attacco DDOS sul server. Un'ottima soluzione per prevenire situazioni di questo tipo sarebbe costruire un cluster di server creando una ridondanza, in modo che in caso di attacco le richieste verrebbero distribuite su più server. Altre soluzioni potrebbero consistere nel configurare un numero massimo di connessioni contemporanee permesse verso l'applicazione in questione.

Domanda 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.

La soluzione più sicura per evitare che il malware che ha infettato il Web Server si propaghi nella rete interna è scollegarlo fisicamente. In figura rappresentiamo questa situazione andando a rimuovere la connessione in blu:



Facendo questo primo step possiamo successivamente andare ad analizzare la situazione sul server collegandoci fisicamente ad esso, ad esempio recandoci in sala server con un pc, senza che il business venga impattato, dato che stiamo ancora permettendo le connessioni da internet sull'applicazione, e senza rischi di propagazione del malware nella rete interna.

Notiamo che un'altra soluzione per isolare dalla rete interna il server sarebbe potuta essere quella di una creazione di una VLAN apposita diversa da quella usata per la rete interna, ma avrebbe avuto un livello di sicurezza minore rispetto all'isolamento fisico in quanto si tratta appunto di una configurazione software.

Ulteriori considerazioni:
Nonostante dopo queste operazioni la rete interna dell'azienda non corra rischi, andiamo a notare che il malware potrebbe potenzialmente infettare anche i clienti legittimi all'applicazione, in quanto la stessa risulta ancora connessa ad internet (e potenzialmente quindi anche all'attaccante). Questo causerebbe un danno di immagine a livello di reputazione non indifferente all'azienda stessa.

Infine per il ripristino completo delle attività, prima di ricollegare il tutto come nella situazione iniziale è necessario andare a rimuovere il malware dal sistema. Se siamo a conoscenza di quando è avvenuto l'evento di immissione del malware, la soluzione migliore è il ripristino tramite backup del codice del server ad una data precedente all'attacco. Idealmente tale operazione andrebbe eseguita fuori dall'orario di operatività dell'azienda, per non impattare sul business.
Se invece non siamo a conoscenza della data dell'evento malevolo, la soluzione più sicura sarebbe quella di sostituire il server con uno nuovo, in quanto anche i backup potrebbero contenere il malware. Il server infetto andrebbe invece formattato o distrutto (a seconda delle policy dell'azienda stilate in fase di analisi della sicurezza).