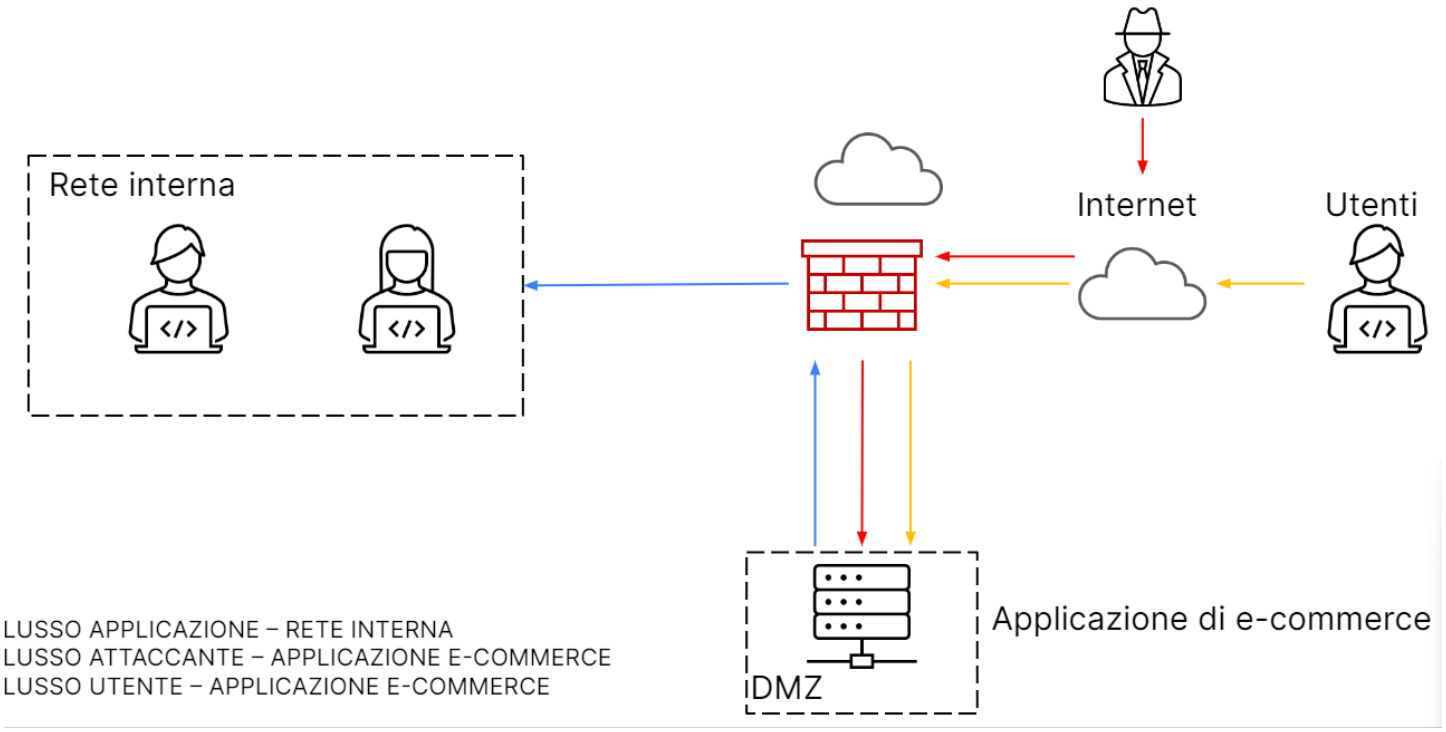
Impatti sul buisness:

l’app web ha subito un DDoS dall’esterno rendendo inutilizzabile l’app per 10 minuti.Considerando una perdita di 1500€ al minuto possiamo calcolare la perdita totale
causata dall'attacco usando la formula SLE(single loss expectancy)
"SLE=AVxEF"
SLE rappresenta il valore delle perdite potenziali da un singolo evento.
AV(asset value) rappresenta il valore dell'asset colpito dall'attacco.In questo caso l'AV potrebbe essere considerato come il valore dei potenziali guadagni persi durante l'attacco.in questo caso 1500€ al minuto x 10 minuti =15000€.
EF(exposure factor) = rappresenta il fattore di esposizione,ovvero quanto l'asset è stato compromesso o esposto dall'evento.In questo caso potremmo dire che lo è al 100% per questo gli verrà assegnato il valore di "1"(intero).
Considerando questi dati possiamo calcolare il nostro SLE:
SLE=AVxEF 15000x1=15000€.

Come azioni preventive consigliate da applicare alla problematica si possono prendere in considerazione:
-implementazione di firewall e regole di sicurezza avanzate per filtrare il traffico dannoso in modo da mantenere l'app accessibile anche se sotto attacco bloccando eventuali attacchi.
-implementazione di soluzioni per il bilanciamento del carico per distribuire il traffico tra più server cosi che se uno è sotto attacco,gli altri possono continuare ad erogare traffico mantenendo il servizio attivo.
-il monitoraggio della rete in tempo reale può aiutare a rilevare tenativi di attacchi e rispondere rapidamente.
E' importante inoltre preparare un incident response plan che definisce un piano di risposta agli incidenti per sapere come affrontare determinate minacce ed agire rapidamente per ripristinare i servizi il prima possibile.

Immagine di base della rete che andremo a modificare:

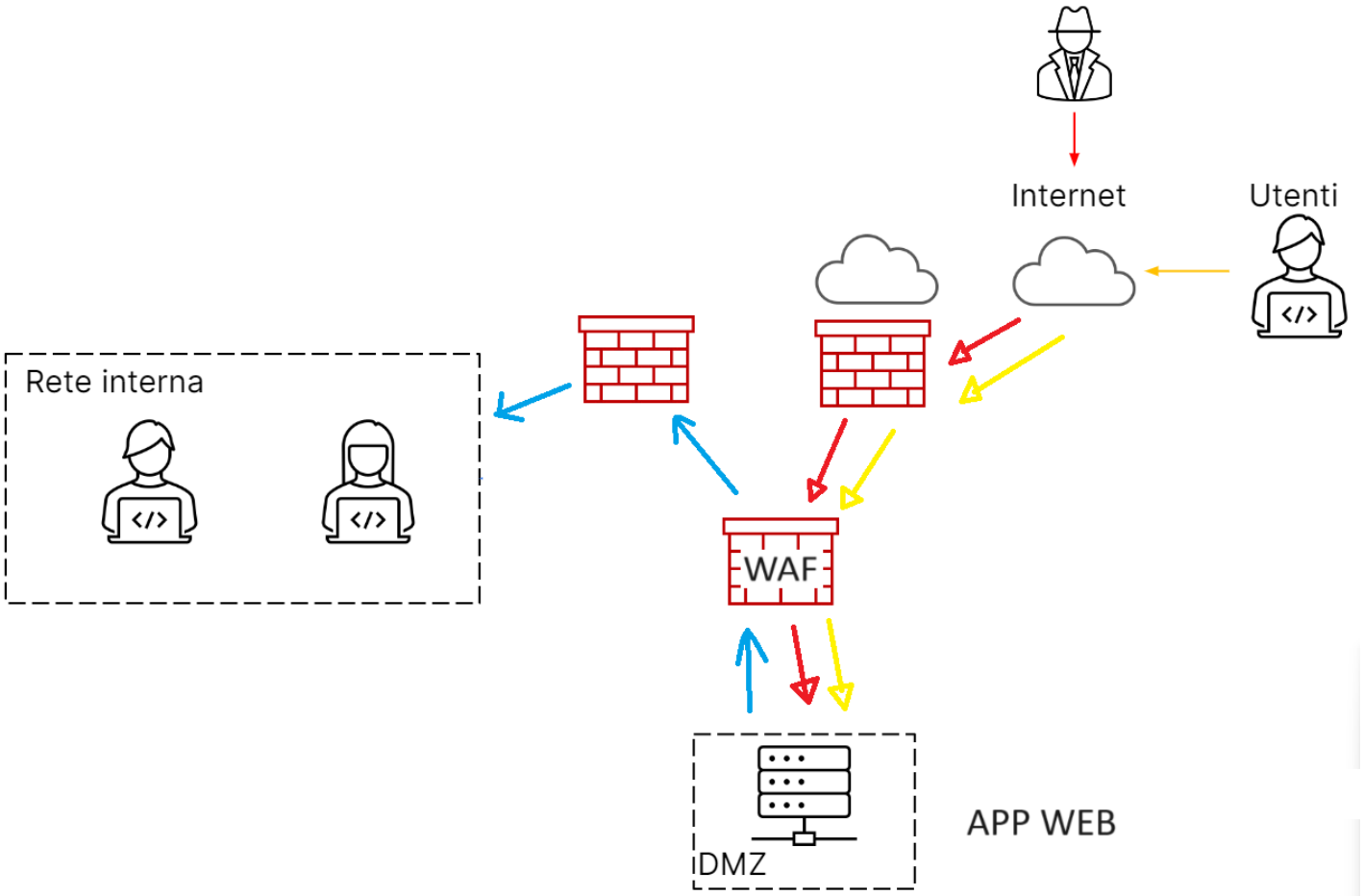


Per difendere un'applicazione web da attacchi XSS e SQLi, è possibile implementare una serie di azioni preventive tra le quali:

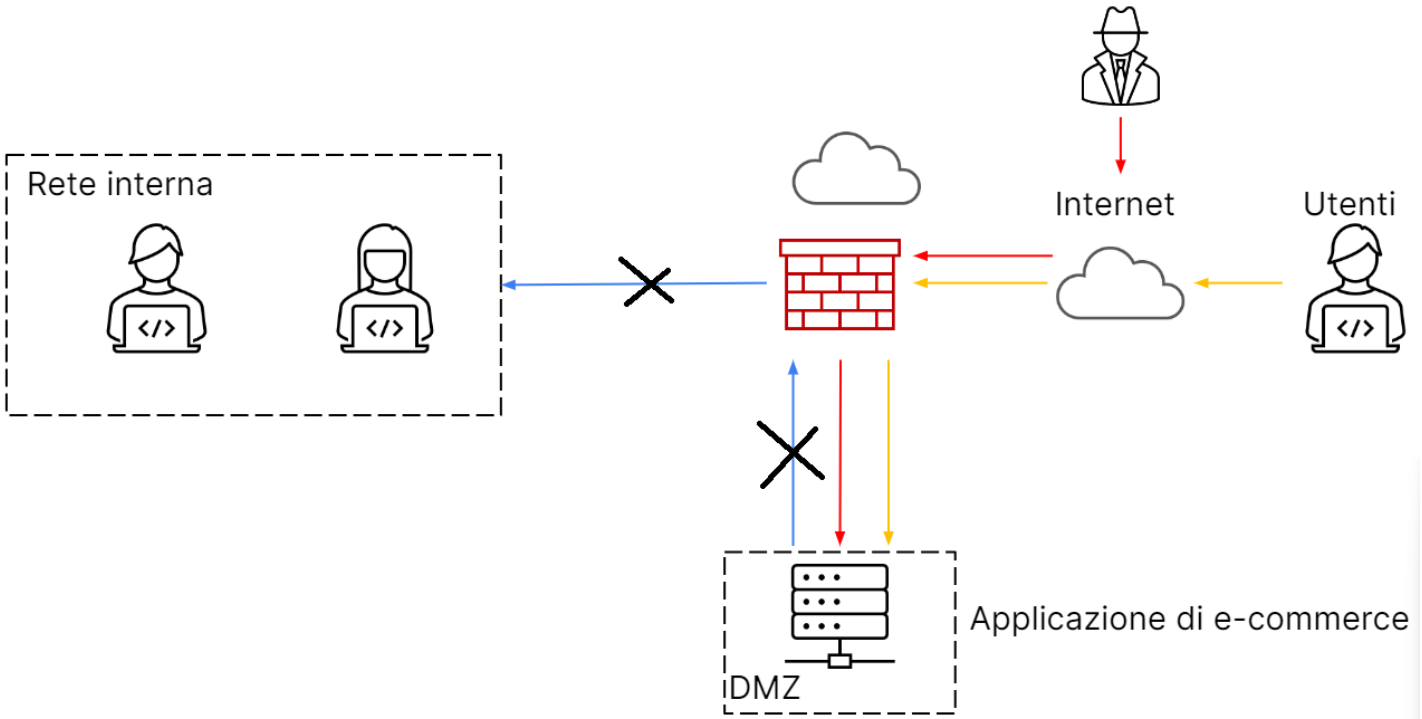
-validazione dei dati in ingresso
-sanitizzazione dei dati
-procedura di gestione degli errori
-WAF(web application firewall).

Quest’ultimo, è un dispositivo o un software che protegge le applicazioni web da varie minacce e vulnerabilità. Il suo scopo principale è quello di filtrare il traffico web in ingresso e in uscita per identificare e prevenire attacchi alle applicazioni web come appunto XSS e SQLi.Un WAF analizza tutto il traffico web che passa attraverso di esso e filtra richieste e risposte per rilevare comportamenti sospetti.Tra le sue altre principali funzioni c’è la “validazione delle sessioni” che assicura che le sessione utente siano autentiche proteggendo da attachi come hijacking.

In figura l’installazione di un WAF che,installato tra il firewall esterno e la DMZ fornisce un’ulteriore protezione sia in entrata che in uscita.



Una delle tecniche preventive per la gestione di incidenti sulla rete è la segmentazione,ossia la suddivisione della rete in lan o vlan. Ciò avviene ad esempio creando una rete ad hoc chiamata generalmente,rete di quarantena,che configurata in modo giusto impedirebbe al malware di riprodursi sulla rete interna. È inoltre possibile ricreare lo stesso scenario configurando in maniera esatta le policy del firewall rivedendo le connessioni in entrata ed uscita.



Sebbene la segmentazione della rete riesce a limitare la riproduzione del malware,spesso,non basta per limitare l'accesso della rete da parte dell'attaccante. Per questo viene implementata una misura di sicurezza maggiore attraverso una tacnica chiamata Isolamento.L'isolamento consiste nella completa disconnessione del sistema infetto dalla rete. Questa soluzione lascia l'attaccante ancora collegato al sistema tramite internet ma non più in grado di riprodursi.

In questa soluzione abbiniamo le azieni preventive(in questo caso il WAF) alla response che nel nostro caso è un azione di segmentazione) che impediscono all'attaccante di raggiungere la rete interna. In questo modo il traffico viene filtrato e protetto sia in entrata che in uscita e non dovrebbe essere possibile per il malware riuscire a moltiplicarsi su altre macchine.
ricordiamo che come soluzione alternativa alla segmentazione c'è l'isolamento che isola completamente la macchina dalla rete .

isolamento