Report – M5W20D5

Ipotesi di difesa da un attacco

Indice generale

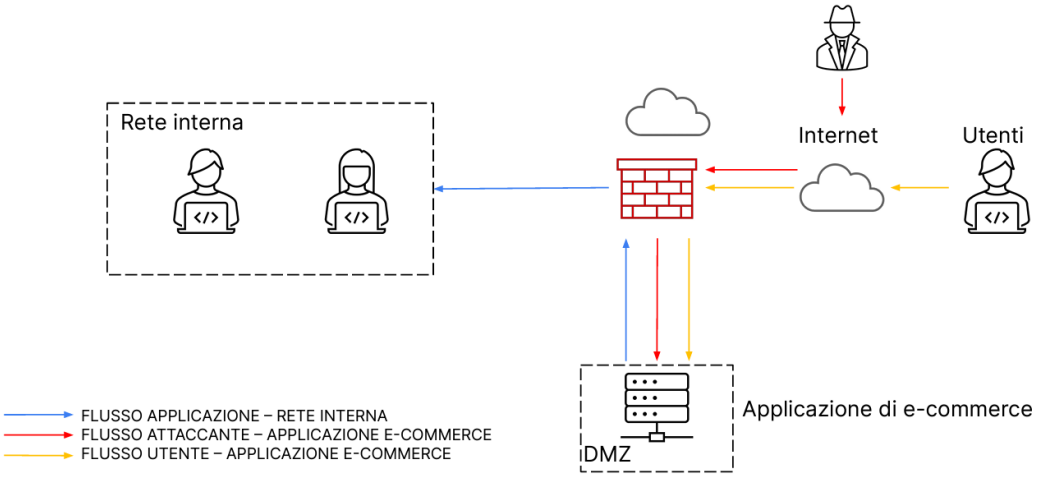
Introduzione e situazione iniziale

Viene mostrata di seguito la schematica rappresentazione di un’azienda che si occupa di e-commerce sotto attacco: un attaccante esterno è riuscito a superare le difese del firewall e ha ottenuto l’accesso al server sul quale è in esecuzione la web-app.

Verranno poste varie richieste e scenari da sviluppare e analizzare per poter progettare un piano di risposta all’attacco.

Architettura di rete:
L’applicazione di e-commerce deve essere disponibile per gli utenti tramite Internet per effettuare acquisti sulla piattaforma.

La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.



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.

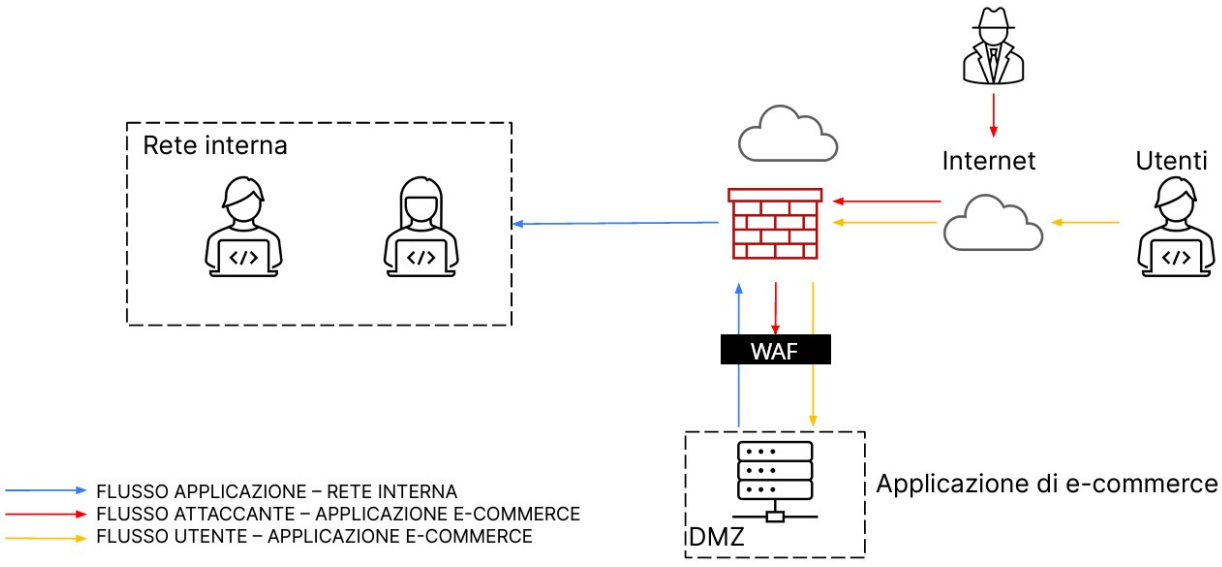
Prima di tutto andiamo a ricordare che gli attacchi SQLi e XSS sono possibili nel caso di una programmazione non ottimale della web-app che permette all'attaccante di utilizzare codice SQL liberamente o caricare codice malevolo.

Una prima soluzione palese è quella di migliorare il codice della web-app sopratutto dove siano richiesti input all'utente, sia sotto forma di testo che di file da caricare, in modo che sia correttamente validato prima di essere eseguito.

Una seconda soluzione è l'utilizzo di WAF o Web Application Firewall, cioè un firewall progettato specificamente per difendere le web-app dagli attacchi, inclusi SQLi e XSS, e per la gestione del traffico internet indesiderato.

Altre soluzioni:

- patch management: controllare che siano state installate le più recenti patch di sicurezza
- software UEBA: è uno strumento per l'analisi di comportamenti e attività sospette che possono suggerire un attacco in corso
- servizi Coud: sfruttare risorse in rete di grandi aziende permette di fare affidamento sulle loro vaste risorse di sicurezza



Impatti sul business

L’applicazione Web subisce un attacco di tipo DDoS dall’esterno che rende l’applicazione non raggiungibile per 10min. Calcolare l’impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media ogni minuto gli utenti spendono 1500€ sulla piattaforma di e-commerce. Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica.

Una attacco DDoS, o distributed denial of service, consiste in un esteso fronte di richieste che portano il server alla totale saturazione e impediscono il suo normale funzionamento.

L’impatto subito dal business, in termini economici, ammonta a 15000€ di mancate vendite nell’arco dei dieci minuti di durata dell’attacco, ma questa non è l’unica perdita: ci potrebbe essere una perdita di immagine, sopratutto se l’attacco si ripete nel tempo, ma anche una perdita di clienti stessi sia per delusione nei confronti dell’azienda che per l’eventuale scoperta/utilizzo di una piattaforma concorrente.

Per quanto riguarda le azioni preventive, anche in questo caso l’utilizzo di specifici firewall è fondamentale, oltre al WAF citato prima un altro candidato è NGF o next-generation firewall: questo strumento mette a disposizione strumenti di analisi della rete e delle applicazioni per individuare situazioni anomale in tempi brevissimi.

Essendo il punto critico la capacità del server di far fronte a una grande mole di richieste, un’altra soluzione consiste nell’implementare un failover cluster, cioè uno o più server secondari che entrano in azione quando il quello sotto attacco non è più in grado di soddisfare il traffico da solo.

Response

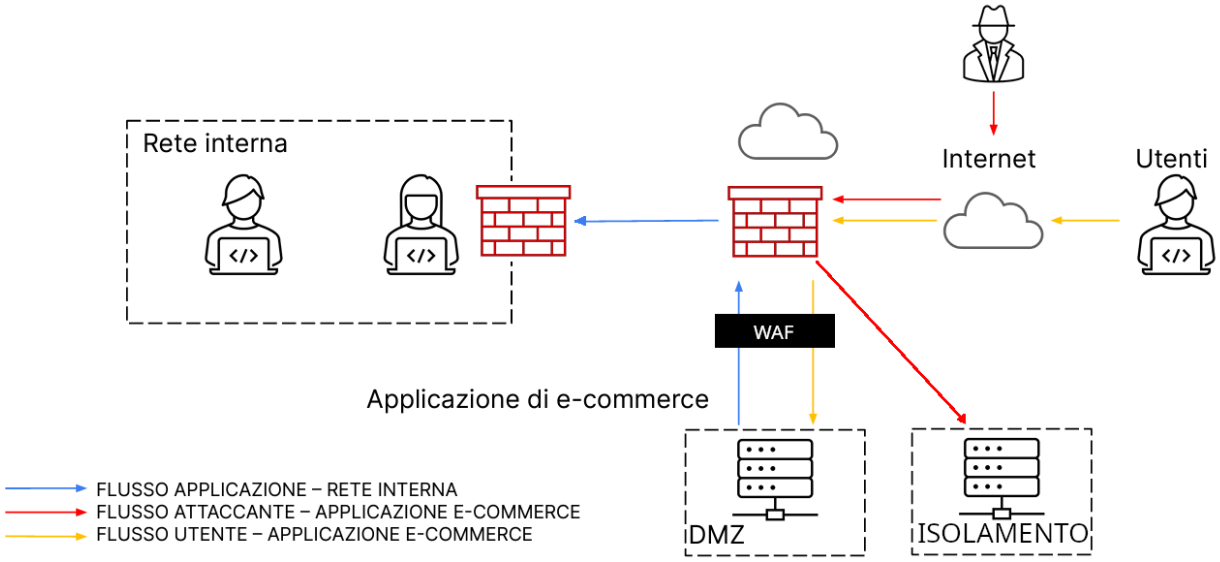
L’applicazione web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostra rete, mentre non siete interessati a rimuovere l’accesso da parte dell’attaccante alla macchina infettata. Modificate la figura con la soluzione proposta.

In questo caso si dovrà operare tempestivamente per isolare il server infetto dal resto della rete segmentandolo in una rete esterna con le giuste configurazioni del router aziendale.

Però con il server in isolamento dobbiamo garantire la continuità del business, sarà quindi necessario che siano disponibili delle soluzioni di backup per ripristinare l’attività, come ad esempio un server secondario dal quale riattivare la piattaforma online.

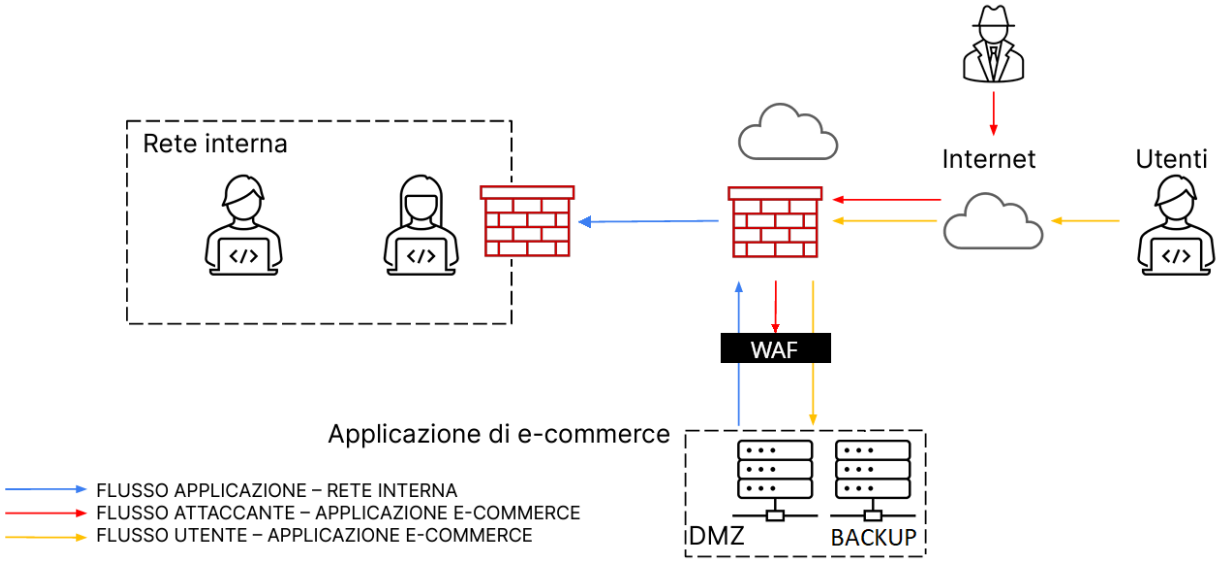
La protezione del resto della rete aziendale può essere migliorata dalla presenza di firewall addizionali preposti alla salvaguardia delle specifiche sezioni in cui è suddivisa la rete aziendale.

Altro fattore importante è l’addestramento e l’aggiornamento dei dipendenti alle possibili minacce sulla rete, in modo che non commettano errori che potrebbero fornire l’accesso non autorizzato all’attaccante.



Soluzione Competa

Unire i disegni dell'azione preventiva e della response.



Modifica "più aggressiva" dell'infrastruttura

Se ritenuto necessario, anche integrando la soluzione della sezione impatti sul business.