Claudio De cicco

23/11/2022

Report

Traccia:

Con riferimento alla figura in slide 2, rispondere ai seguenti quesiti.

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

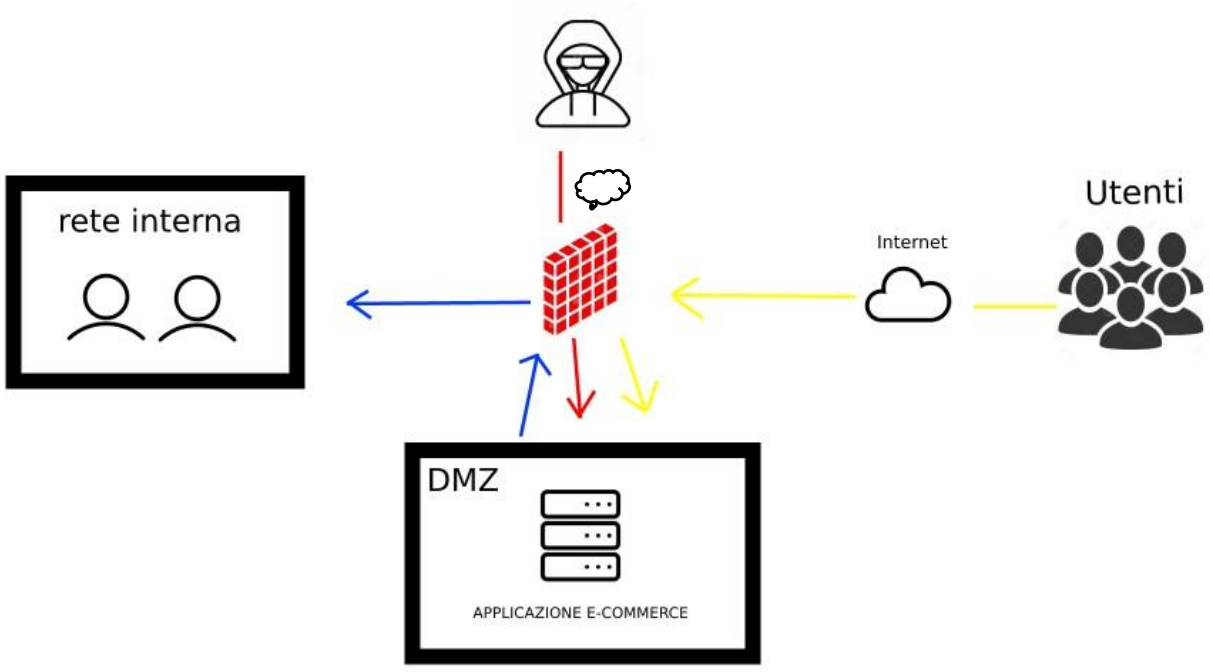
2. **Impatti sul business**: l'applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione non raggiungibile per **10 minuti**.
   Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media **ogni minuto gli utenti spendono 1.500 €** 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.

4. **Soluzione completa**: unire i disegni dell'azione preventiva e della response

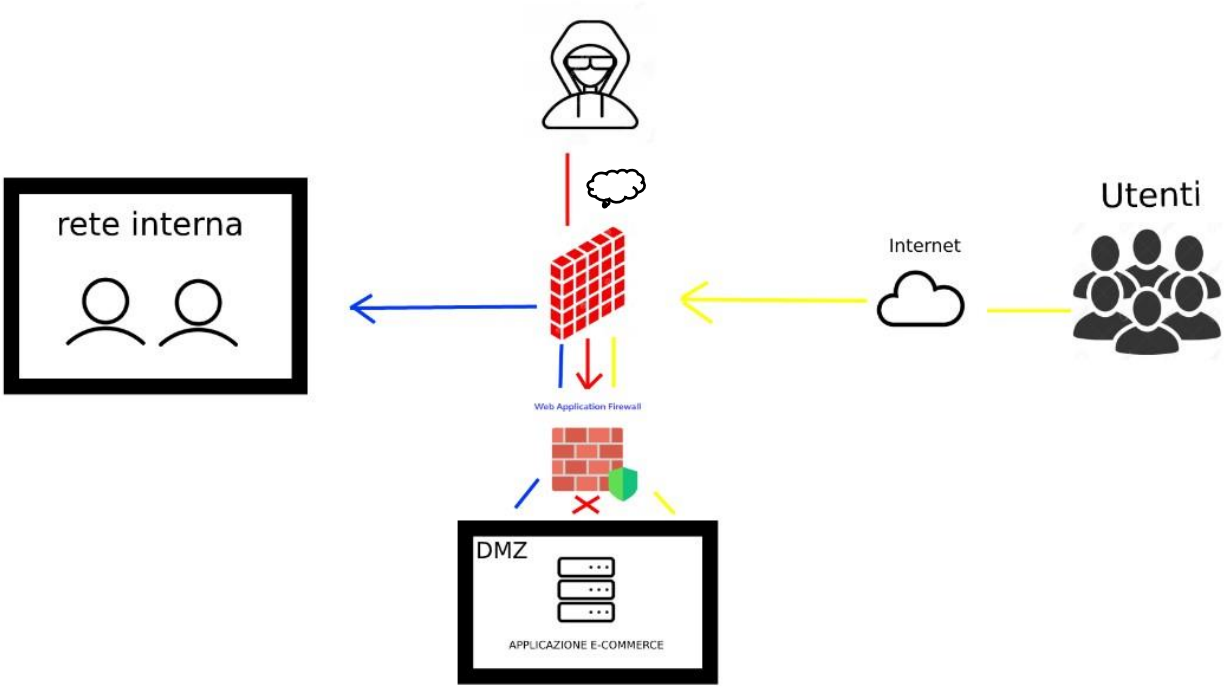
5. **Modifica «più aggressiva» dell'infrastruttura (se necessario/facoltativo)**

Questa è la rete di partenza:



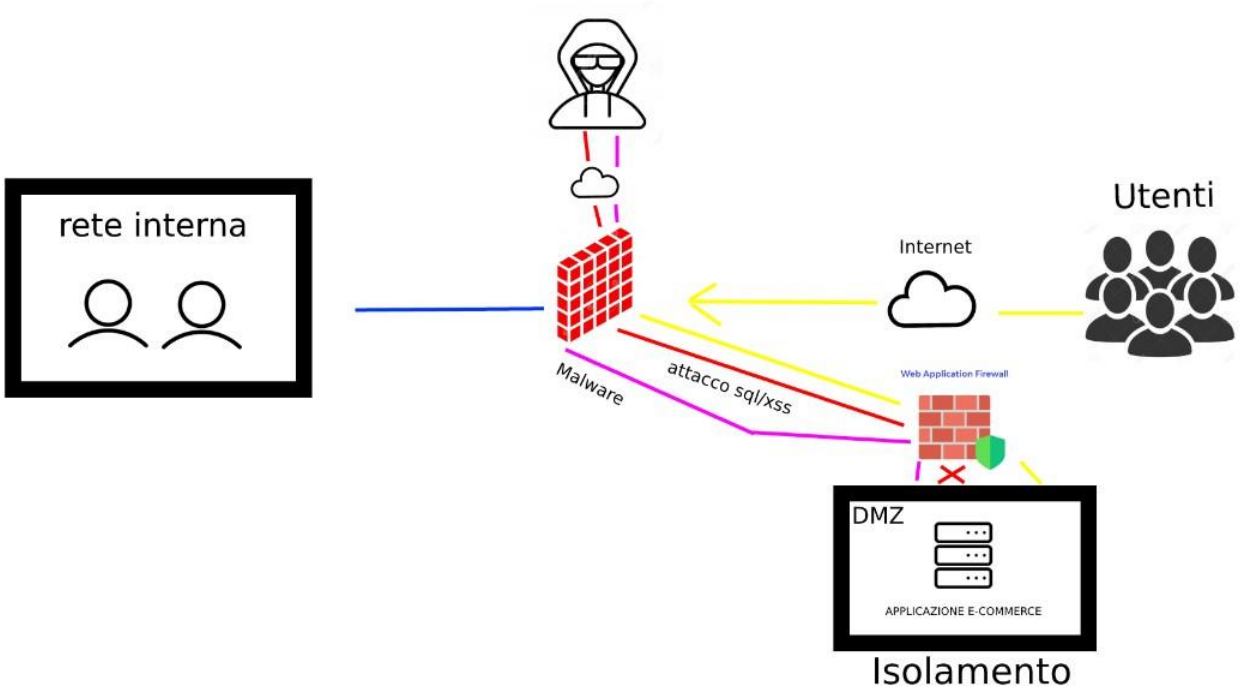
Punto 1 – Come possiamo notare la nostra applicazione potrebbe essere attaccata da attacchi di tipo sql o xss. Come misura preventiva quindi andiamo ad aggiungere un WAF (web application firewall) firewall che lavorano al livello 7 (applicativo) della pila ISO/OSI.Fondamentalmente ispezionano il traffico HTTP in entrata (e volendo anche in risposta), assegnano un punteggio di pericolosità alla richiesta e, superato il livello di attenzione previsto, la

bloccano.Una richiesta bloccata non viene nemmeno eseguita dall'applicazione web (e si evita a monte che quest'ultima non sia in grado di gestirla).



Punto 2 – In questo caso andremo a calcolare le perdite moltiplicandole per i minuti che il server è stato offline. Quindi andiamo a fare 1.500 (media spesa dagli utenti al minuto) per i 10 minuti in cui il servizio è stato irraggiungibile. L'azienda avrà una perdita di **15.000 euro**. In questo oltre alla perdita dal punto di vista economico va considerato anche l'impatto che subirà l'azienda dalla "pubblicità" negativa dell'accaduto , perdento fiducia e affidabilià per alcuni clienti.

Punto 3 - In questa situazione ci troviamo ad essere infettati e quello che vogliamo fare è scollegare l'applicazione dalla nostra rete interna ma non da internet , quindi andremo ad isolare la nostra web application.



Come possiamo vedere abbiamo isolato l'applicazione dalla rete interna, ma non da internet , in questo modo non diamo la possibilità all'attaccante di poter entrare nella nostra rete interna ma di mantenere però l'accesso alla macchina infettata.

Punto 4 – Come possiamo vedere nell'ultima immagine la nostra applicazione e-commerce risulta essere protetta da attacchi di tipo sql/xss tramite l'istallazione di un WAF , e risulta anche essere scollegata dalla rete interna perché infettata da un malware.