Giacomo Manca - Epicode

Incident response

27 Novembre, 2023

Introduzione

Lo scopo di questo progetto è di illustrare le contromisure da prendere nel caso di un ipotetico attacco informatico ad un'azienda attiva nell'e-commerce, e di fare una stima dei costi e perdite che l'azienda andrebbe ad affrontare.

Obiettivi

1. Indicare le azioni preventive che si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato.

2. 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. Si supponga un'interruzione dei servizi di 10 minuti.

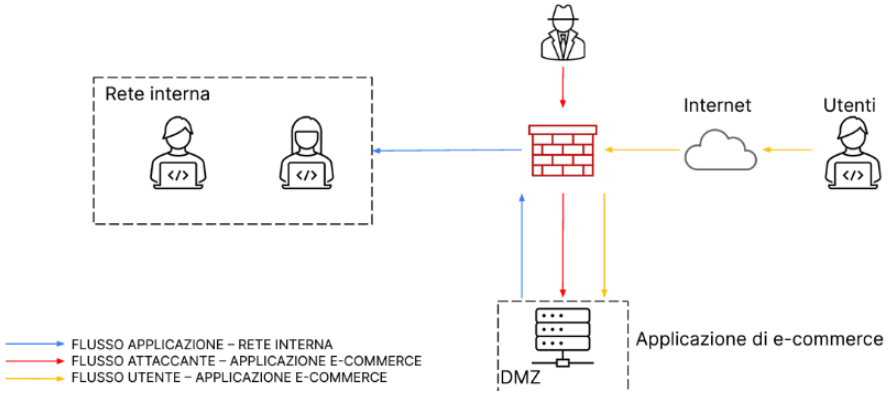
3. Indicare le contromisure efficaci nel caso in cui l'applicazione Web venga infettata da un malware. La priorità è che il malware non si propaghi sulla rete interna.

1. Azioni preventive

La situazione di partenza è la seguente:

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

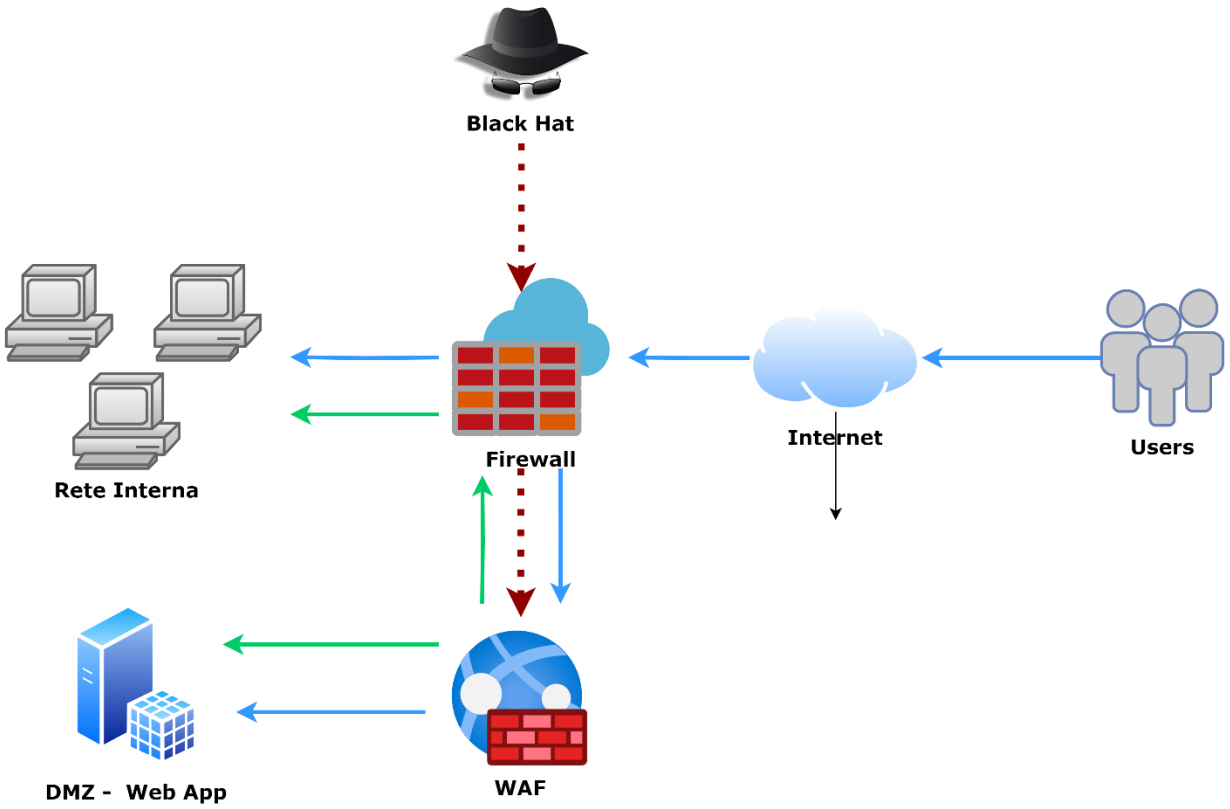
La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.



Le misure più indicate ed efficaci per proteggere la web-app da attacchi di tipo SQL e XSS sono le seguenti:

- Effettuare una valida validazione e sanitizzazione degli input dell'utente. Limitare e filtrare gli input in modo da accettare solo dati attesi e sicuri.
- Utilizzare sempre query SQL parametrizzate.
- Rimuovere o codificare caratteri speciali che potrebbero essere utilizzati in attacchi XSS.
- Implementare un WAF per filtrare e monitorare il traffico HTTP tra un'applicazione web e l'Internet. Può aiutare a rilevare e bloccare attacchi SQLi.

L'immagine seguente descrive la nuova architettura con il WAF implementato a difesa della web app.



2. Impatti sul business

Per calcolare l'impatto finanziario sul business dovuto a un attacco DDoS che rende l'applicazione non raggiungibile per 10 minuti, puoi utilizzare la seguente formula:

(Perdita di Ricavi per Minuto)×(Durata dell'Interruzione in Minuti)

Dato che in media ogni minuto gli utenti spendono 1.500 €, possiamo quantificare la perdita di ricavi stimata durante il periodo di interruzione in 15.000 €.

3. Incident response

Al fine di impedire che un malware si propaghi in una rete, l'azione di **isolamento** è una soluzione. Questa strategia prevede l'isolamento di parti compromesse del sistema o della rete per evitare che l'attacco si diffonda ad altre aree.
Nel nostro caso specificio andremo ad isolare la rete interna, per evitare che l'attaccante possa penetrarla. Una volta isolata la rete interna, si potrà andare ad operare sulla rete infettata. Questa strategia non andrà però a proteggere gli utenti che utilizzeranno la piattaforma di e-commerce. Il malware potrà infatti propagarsi fino a che questa non viene sanificata. Sarebbe opportuno isolare contestualmente anche la web-app, tuttavia questo inciderebbe sui costi da sostenere.