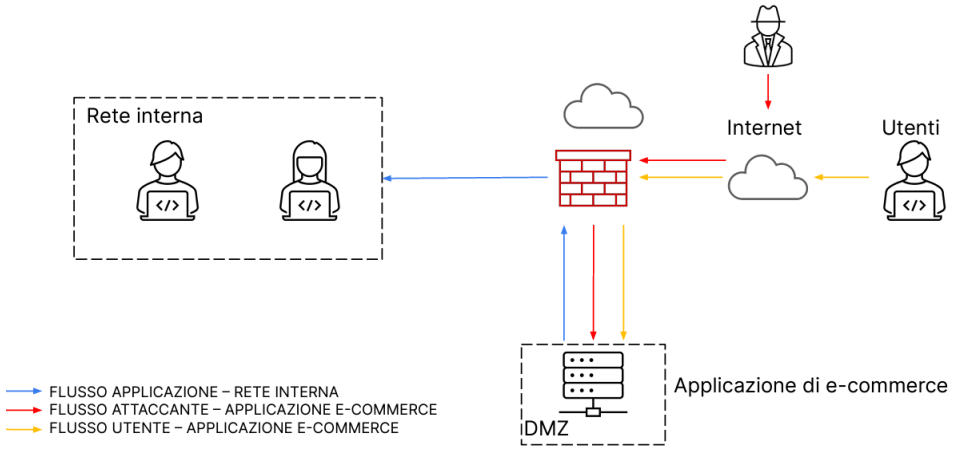
Esercitazione W20D4

Ilaria Pedrelli

Progetto fine modulo 5

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.



- ## Svolgimento punto numero 1

Al fine di mitigare il rischio di attacchi attacchi XSS o SQLi ci sono diverse azioni preventive che possiamo implementare, tra cui:

Piani di Vulnerability assessment e pen test periodici in modo da ridurre il rischio su un sistema a valle. Cicli e sessioni di PT sugli end-point possono coprire eventuali vulnerabilità implementando le azioni di rimedio.

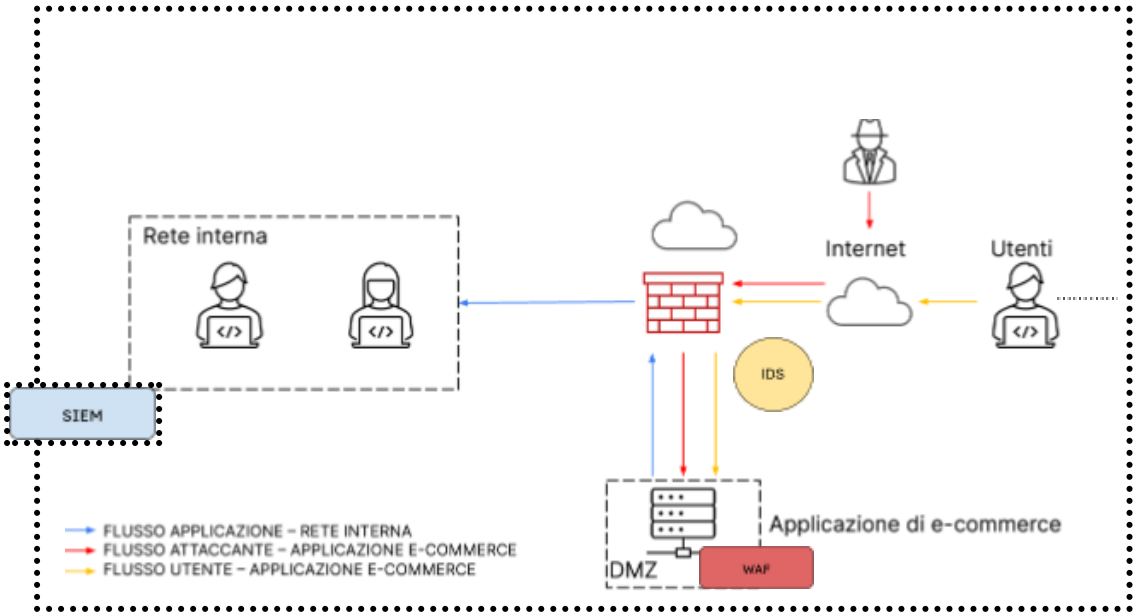
Sanitizzazione dei dati di Input e Output quindi, eliminare eventuali caratteri speciali, sequenze o altri elementi che potrebbero essere utilizzati per eseguire attacchi di tipo SQLi o XSS sia nella fase di elaborazione e memorizzazione dei dati degli utenti, sia nella fase di restituzione e visualizzazione di quest'ultimi per evitare esecuzione di codice dannoso. Inoltre, è importante anche garantire che i dati in input garantiscano determinati criteri di lunghezza e conformità.

Implementare un sistema di monitoraggio e logging che permettono di tracciare tutte le azioni sulla web app. Tramite i log applicativi, è possibile individuare tentativi di attacchi SQLi, XSS e tentativi di accesso non autorizzati oltre a fornire una traccia degli eventi a incidente avvenuto.

A questo proposito, è di fondamentale importanza un SIEM per il monitoraggio e la gestione dei Log. Il SIEM permette di centralizzare i Log in un unica piattaforma semplificando il processo di monitoraggio e analisi e per avere una visione più precisa delle attività anche ad attacco avvenuto.

Un altro approccio preventivo è quello di **inserire un sistema di prevenzione e rilevamento delle intrusioni** per individuare preventivamente potenziali attacchi e che permette di monitorare comportamenti sospetti. In questo caso inserire un IDS tra il Firewall e la DMZ permetti di avere un ulteriore controllo dopo il filtraggio del Firewall. In questo modo, con le giuste policy, L'IDS può segnalare al firewall di bloccare una minaccia prima che raggiunga la rete interna.

Per ultimo, Implementare anche un altro tipo di **Firewall** apposito per proteggere le applicazioni da attacchi XSS e SQLi cioè il **WAF (Web Application Firewall**, installato direttamente all'interno della DMZ per filtrare e monitorare il traffico in ingresso e in uscita, identificando e bloccando eventuali attacchi.



- ## Svolgimento punto numero 2

L'applicazione Web ha subito un attacco di tipo DDoS per 10 minuti perdendo di fatto entrate monetarie alla piattaforma per 15.000 euro dato che, in media, l'applicazione registra guadagni per 1.500 euro al minuto.

Anche in questo caso tra le azioni preventive rientrano **SIEM e sistemi di monitoraggio** come IPS e IDS ma anche utilizzo di **sistema anti-DDoS** I sistemi anti-DDoS sono servizi specializzati nella mitigazione di questo tipo di attacchi. Un esempio potrebbe essere il servizio protezione DDoS offerto da Microsoft (Azure) che, in combinazione con un WAF, offre protezione sia ai livelli 3 e 4 che al livello di applicazione cioè il livello 7.

Un'ulteriore azione potrebbe essere quella di **implementare un Disaster recovery as a service (DRaaS)** che permette di attivare immediatamente una infrastruttura in cloud in caso di attacco e quindi di ripristinare il servizio in meno tempo e di mantenerlo attivo fino al totale ripristino dei server infetti. L'aspetto migliore di questa azione è che i servizi di questo tipo vengono pagati solo per il loro utilizzo.
Ovviamente ci sono aspetti da valutare prima di implementare questo tipo di azione come il tempo di switch dell'intera rete e il costo del servizio al minuto. Il tempo di switch e il costo del servizio non dovranno superare l'impatto ipotetico sul business che l'azienda potrebbe avere nel caso di uno "stop" dei servizi causato da un attacco DDoS.

- ## Svolgimento punto numero 3

L'applicazione è stata infettata da un malware. Il primo step per contenere l'impatto nel caso un componente sia stato infettato da un malware, è l'isolamento del sistema. in questo caso della DMZ, in modo tale che non infetti anche la rete interna. L'azienda ha ritenuto opportuno mettere in atto la tecnica dell'**isolamento** e quindi, isolare il server DMZ. In questo scenario però l'attaccante avrebbe ancora accesso al sistema tramite internet.

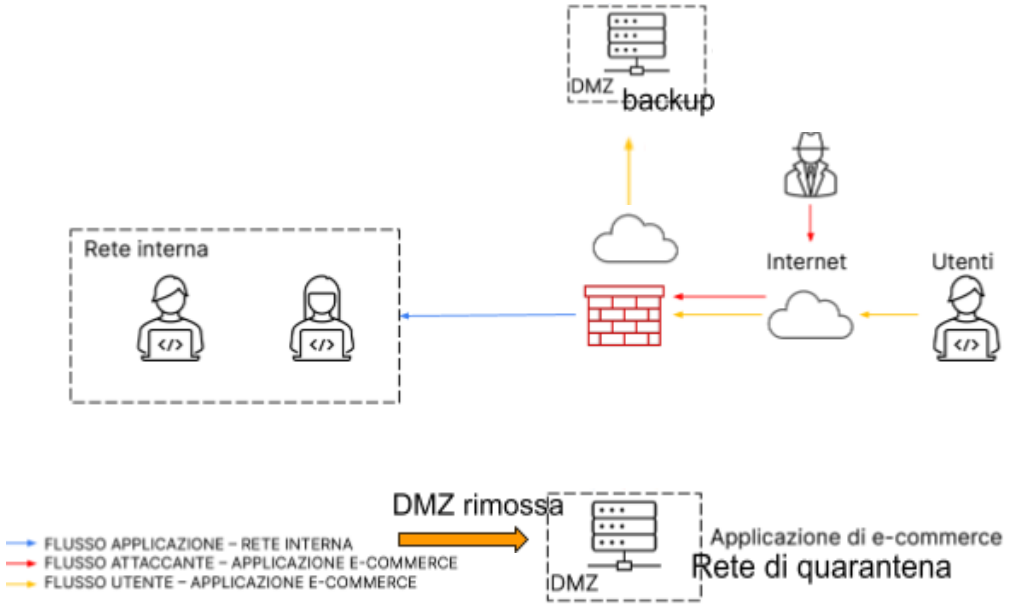
- ## Svolgimento punto numero 5

Per mettere in atto un sistema di contenimento più stringente, si può utilizzare **la rimozione** del sistema infetto dalla rete sia interna che da internet ed illustrata nel disegno seguente.

Precedentemente come azione preventiva, è creato un **server di backup** della DMZ dalla quale posso ripristinare i dati e mantenere attiva la web app senza danni al business e con una strategia di full backup per evitare di perdere qualsiasi tipo di dato.

Inoltre, è opportuno che l'azienda implementi anche un **backup In Cloud** con un service provider esterno come Amazon o Microsoft con quella parte di dati considerati meno critici.

La figura seguente mostra sia l'isolamento della componente infetta dalla rete sia, la rimozione con la messa in quarantena del server infetto.



Svolgimento punto numero 4

Soluzione Completa dei punti 1 e 3