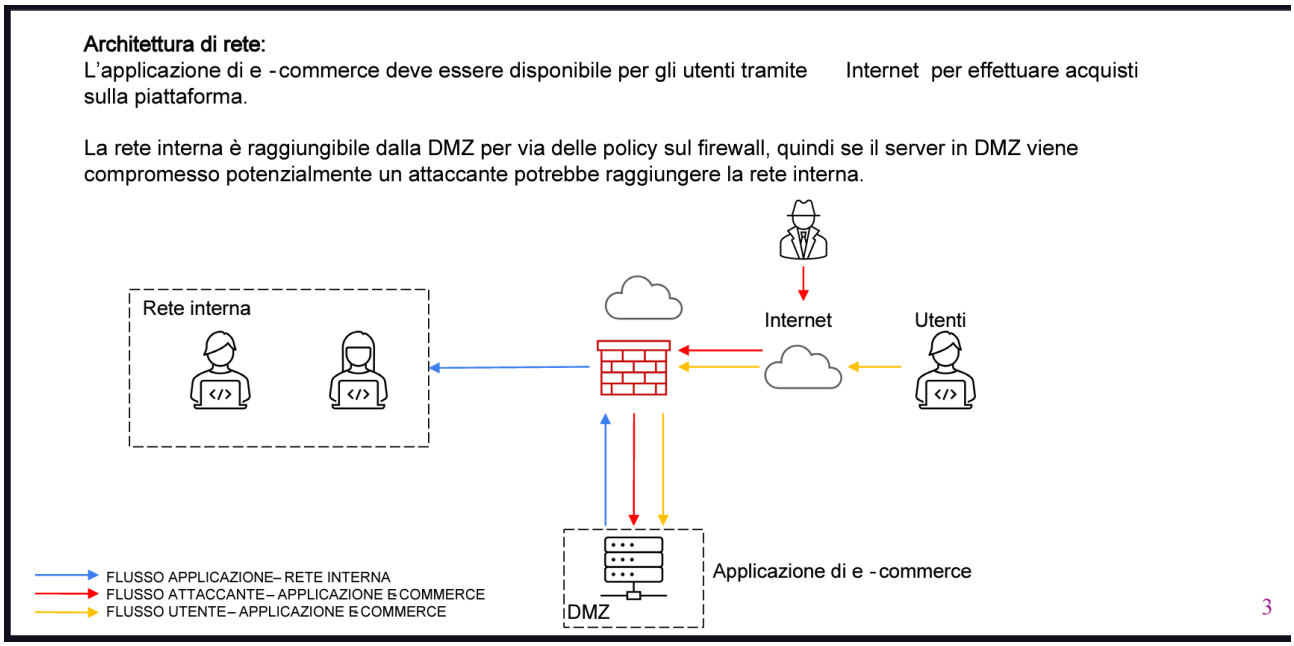
Schema di rete aziendale iniziale:



Azioni preventive:

Definizione attacco XSS

Un attacco XSS (Cross-Site Scripting) è una vulnerabilità informatica che consente a un aggressore di inserire codice malevolo all'interno di una pagina web o di un'applicazione web che sarà poi eseguito sul dispositivo o nel browser dell'utente finale. Questo codice malevolo può essere utilizzato per vari scopi dannosi, tra cui il furto di informazioni sensibili dell'utente (come le credenziali di accesso), la modifica del contenuto della pagina web, il reindirizzamento dell'utente verso siti dannosi o per eseguire azioni non autorizzate a nome dell'utente. Gli attacchi XSS sfruttano spesso lacune nella gestione delle input da parte del server web, consentendo agli aggressori di inserire script dannosi, solitamente scritti in JavaScript, all'interno delle pagine web. Gli attacchi XSS possono essere suddivisi in varie categorie, tra cui XSS riflessi (dove il payload viene eseguito quando l'utente visita un URL compromesso) e XSS memorizzati (dove il payload viene memorizzato nel server e viene eseguito quando altri utenti accedono al contenuto dannoso). Gli attacchi XSS possono avere gravi conseguenze per la sicurezza e l'integrità delle applicazioni web, nonché per la privacy e la sicurezza degli utenti finali.

Definizione attacco SQLi

Un attacco SQLi (Structured Query Language Injection) è un tipo di attacco informatico che sfrutta le vulnerabilità di sicurezza nelle applicazioni web per eseguire comandi SQL non

autorizzati sul database sottostante. Questo tipo di attacco si verifica quando un'applicazione web non valida o filtra correttamente le input fornite dagli utenti, consentendo agli aggressori di inserire codice SQL dannoso all'interno delle query inviate al database.

Gli attacchi SQLi possono avere diverse forme e scopi, tra cui:

1. Estrarre informazioni sensibili dal database, come nomi utente, password o dati personali.
2. Modificare o eliminare dati nel database.
3. Assumere il controllo completo del database o del sistema sottostante.

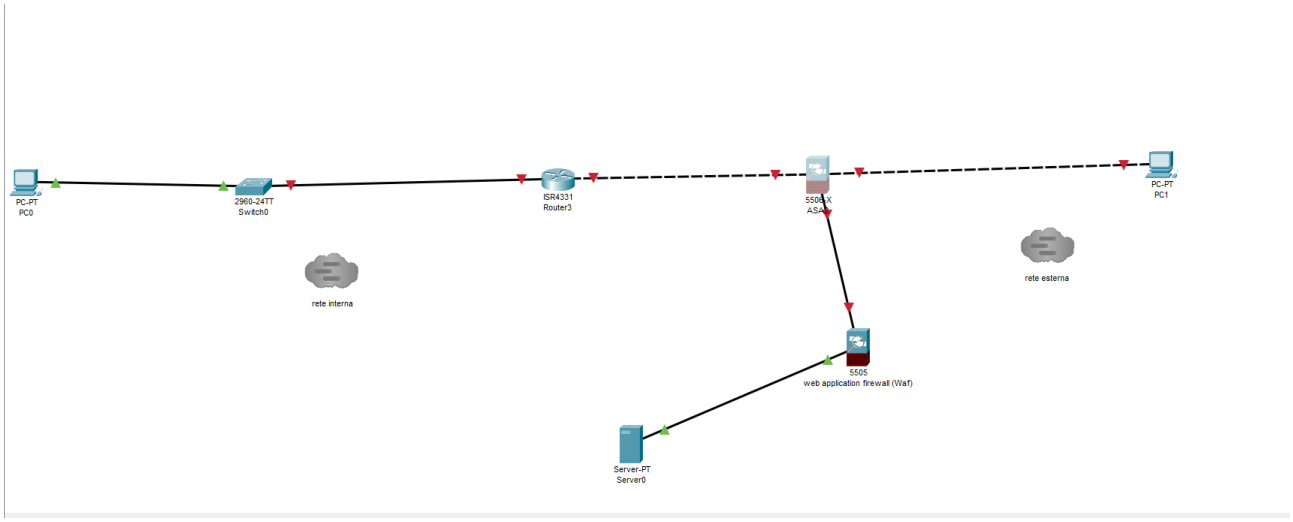
Gli attacchi SQLi possono essere suddivisi in diverse categorie, inclusi attacchi basati su errori di sintassi SQL, attacchi basati su input non validati e attacchi basati su manipolazione degli URL. Gli sviluppatori web devono implementare adeguate pratiche di sicurezza, come l'uso di prepared statements o l'implementazione di ORM (Object-Relational Mapping), per mitigare il rischio di attacchi SQLi.

prevenzione da attacchi di tipo XSS ed SQLi.

se si osserva lo schema di rete sopra riportato si può notare che c'è un collegamento diretto tra rete interna e Dmz il che rappresenta una debolezza agli attacchi di tipo SQLi oppure XSS.

Per poter aumentare il livello di sicurezza di rete della web application si consiglia di aggiungere un WAF (Web Application Firewall) che permette all' azienda di tutelarsi maggiormente dagli attacchi sopra citati (SQLi e XSS).

Qui sotto viene riportata una immagine che rappresenta il nuovo schema di rete.



In questo schema si blocca anche un collegamento rapido tra dmz e rete interna.

Impatti sul business in caso di attacco DDOS

Breve definizione attacco DDOS

Un attacco DDoS (Distributed Denial of Service) è un tipo di attacco informatico in cui un vasto numero di dispositivi, spesso computer o dispositivi Internet of Things (IoT), inviano un'enorme quantità di richieste a un determinato server, sito web o servizio online. Lo scopo di questo attacco è sovraccaricare il sistema bersaglio con un traffico di dati così elevato da renderlo incapace di rispondere alle richieste legittime dei suoi utenti o clienti. L'aggettivo "distribuito" deriva dal fatto che gli attacchi DDoS coinvolgono spesso una rete di dispositivi compromessi, chiamati botnet, controllati da un singolo aggressore o da un gruppo di hacker. Gli attacchi DDoS, dunque, se vanno a buon fine mandano offline un server.

Analisi impatti sul business in caso di attacco DDOS

Se si effettua un'analisi a partire dai dati attuali che riportano che in media gli utenti al minuto 1500 euro. Un eventuale attacco DDOS comporterebbe alla azienda una perdita pari a circa 15000 euro (1500 x 10= 15000).

Azione Response

La strategia da adottare nel Caso in cui il server dell'applicazione web venga infettato da un malware è quella dell'isolamento, visto che la priorità assoluta è quella di evitare che il malware si propaghi nella rete interna. In questo modo si sospende il collegamento rete interna (come si vede in figura da notare come la rete interna sia totalmente scollegata dal server), per evitare che il malware possa in qualche modo andare a diffondersi nella rete interna. Così facendo si limita evita che malware possa permettere all' attaccante di avere accesso alla rete interna e compromettere ulteriormente l'azienda.

Questo pero non vieta alla rete interna di continuare ad proseguire il lavoro.

Per eliminare la minaccia procedere con il ripristino di un backup e bandendo l'indirizzo ip dell' attaccante oltre ad impostare una regola firewall che limita l'accesso al server in questione mantenendo tutto online spostando tutto su un altro server