AZIONE PREVENTIVE PER SQLI INJECTION:

1.) aggiungere un firewall WAF a protezione della Web App. Il WAF si basa su un elenco di firme aggiornate per filtrare le query dannose (e altre minacce online).

2) Effettuare una scansione costante della Web App attraverso un tool di Vulnerability Assessment come Burp Suites.

3.) Convalidare l'input dell'utente e sanitizzarlo (in particolare per XSS)

4.) Effettuare formazione sul personale.

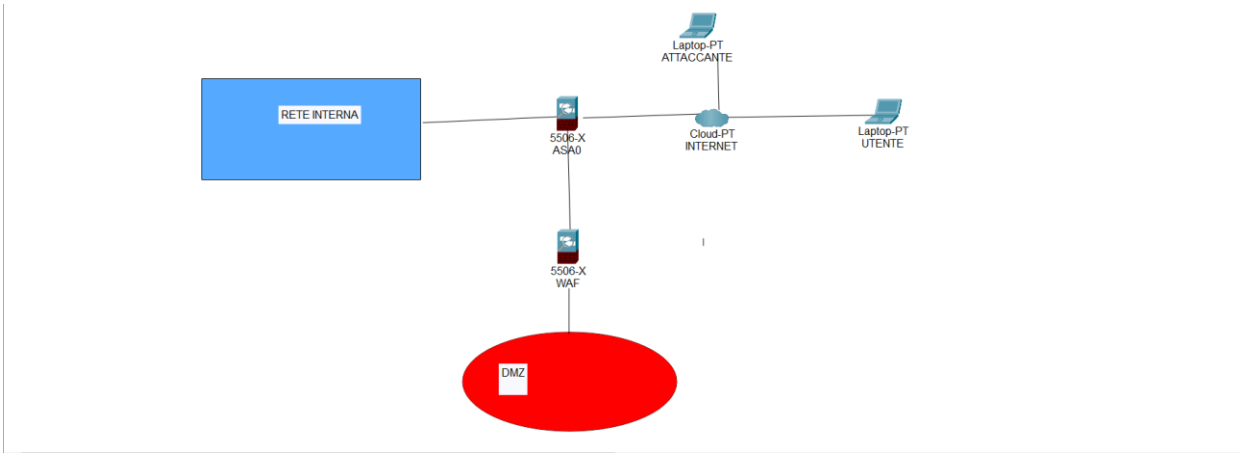
5.) Essere sempre al passo con le ultime versioni aggiornate di software e applicativi (browser, antivirus, etc)

6.) In modo particolare per il XSS, secondo la guida OWASP, occorre controllare estensivamente tutti gli input dell'utente tramite librerie apposite, soprattutto:

A) Nel caso sia necessario riflettere input HTML nella pagina, allora encodarlo tramite HTML ENTITY, usare URL encoding se si riflette url nella pagina. Verificare che i link siano HTTP o HTTPS, e che non si adotti un URI SCHEME come "javascript:" o "data:" (nel caso si accettino link)

B) In caso vi siano API/JASON, controllare che il contenuto sia restituito con Content-type come Application/jason e NON come "text/html"

C) Usare il flag HTTPONLY per evitare l'appropriazione dei cookie da parte dell'attaccante.



IMPATTI SUL BUSINNESS:

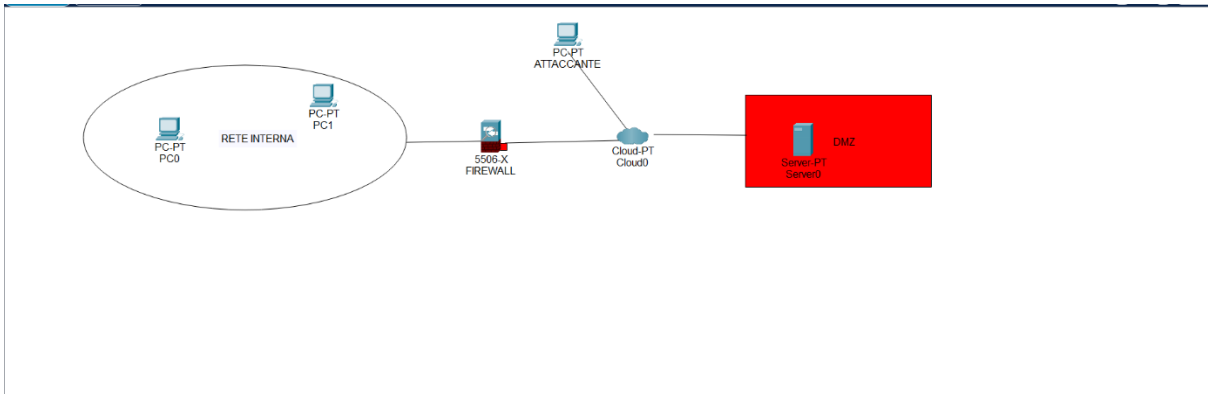
1.500 € x 10 = 15.000 €

Gli impatti sul business in termini economici sarebbero circa di 15.000€ per 10 minuti di inattività, dato che in media ogni minuto vengono spesi circa 1.500€ sulla piattaforma di e-commerce. Tale impatto potrebbe aggravarsi dal fatto che un cliente non potendo acquistare sulla piattaforma, si rivolge al diretto concorrente o comunque acquistare altrove il prodotto portando alla perdita del cliente per acquisti futuri. Ma ricordiamo che gli impatti non sono solo economici, infatti tale inattività potrebbe anche ripercuotersi in termini di pubblicità negativa dell'azienda, sfiducia che si potrebbe generare nei clienti verso l'azienda stessa, oppure possono sorgere anche delle responsabilità etiche/sociali per certi tipi di aziende.

Per prevenire questi scenari, occorre un PIANO DI CONTINUITA' OPERATIVA. In Generale contribuiscono in tal senso, tutte quelle azioni volte ad aumentare la resilienza dei sistemi e la tolleranza agli errori con l'aggiunta di elementi ridondanti all'interno dell'architettura (es. un disco fisso in più per il back up dei dati, magari tramite la configurazione RAID, oppure con l'aggiunta di server nel cosiddetto FAILOVER CLUSTER, o anche con l'aggiunta di generatori di corrente autonoma). Altro elemento da prendere in considerazione per prevenire questi eventi è la scelta della metodologia di salvataggio dei dati (se full,incremential, o differential back up, oppure la migrazione verso il cloud) ricordando che si può optare anche per una scelta ibrida. Infine anche valutare l'azione più efficace ed efficiente nel caso si verifichi un disastro per tornare ad essere operativi sostituendo i componenti compromessi, optando tra diverse soluzioni come cold/hot/warm site, virtualizzare i server sostituendo quelli fisici compromessi, usare il servizio cloud, oppure una soluzione ibrida tra quelle proposte.

RESPONSE

In questo scenario, come azione preventiva si potrebbe intanto attuare una segmentazione della rete in diverse LAN/VLAN permettendo subito di separare il PC infetto creando una rete apposita chiamata rete di quarantena, evitando un eventuale riproduzione del malware essendo separato dal resto della rete. Spesso però tale azione risulta insufficiente, per cui nel nostro caso andremo ad attuare un'azione di isolamento, disconnettendo il server infetto dalla rete interna ma consentendo all'attaccante di accedere alla DMZ tramite internet.



SOLUZIONE COMPLETA

Il server infetto viene isolato dalla rate interna, ma consentiamo comqunque l'accesso alla DMZ all' attaccante e utenti tramite internet. In questo modo il malware non si propaga sulla rete interna e nel frattempo si possono mettere in atto delle remediation actions.