PROGETTO W20

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?

Per proteggere un'applicazione via web, basta impostare bene un web firewall, che sono diversi dai firewall normali perché questi sono progettati per proteggere meglio una applicazione web.

Impatti sul business: Essendo una azienda che lavora con base nel e-commerce, se questo subisce un attacco DDoS e il sito viene giù per qualche ora, oppure giorni, l'azienda perde tantissimi soldi, anche perché parlando di una azienda che lavora solo con base nel e-commerce, il suo guadagno viene principalmente dalla sito web. Quindi possiamo fare un calcolo semplice per vedere l'impatto di questo attacco calcolando i minuti che il sito viene lasciato giù (10min) per il tanto che ogni utente spende nel sito (1500€).

Impatto nel business = 10min * 1500€ = 15000€ che l'e-commerce perde in 10 minuti.

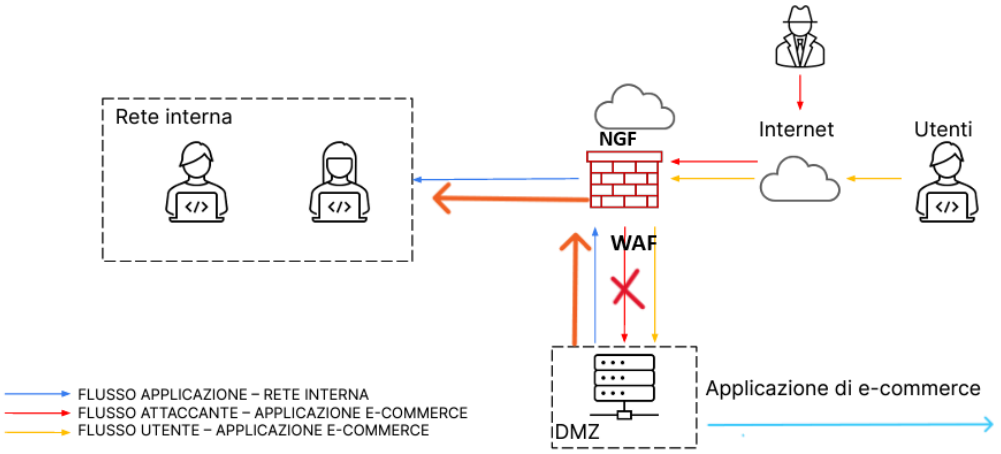
Per risolvere questo problema la soluzione più semplice sarebbe che questa azienda avessi tanto un e-commerce, ma anche una rivendita fisica, oppure essere un fornitore per qualche negozio fisico, se no, può avere un sito di riversa, nel caso uno viene attaccato, quest'altro parte subito come una specie di "nuova"azienda.

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.

Con questo io posso scollegare la mia macchina dalla rete interna, quindi andare a collegare su internet normale, cosi faccio un isolamento della macchina, non lascio vulnerabile il mio DMZ, e posso andare in cerca di cosa sta provando ad attaccare, e magari chi sta attaccando.

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.



Nella freccia blu che esce dal DMZ verso sinistra possiamo mettere un server come secondo backup, un sito di backup come proposto nella soluzione, un salvataggio in Cloud e magari essere un "rivenditore