Esercizio 24-03

Traccia: facendo riferimento alla figura qui sotto, rispondere ai seguenti quesiti:

1. Azioni preventive: quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQL oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni

2. Impatti sul business: l'applicazione Web subisce un attacco di tipo DdoS dall'esterno che rende l'applicazione non raggiungibile per 10 minuti. 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. Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica.

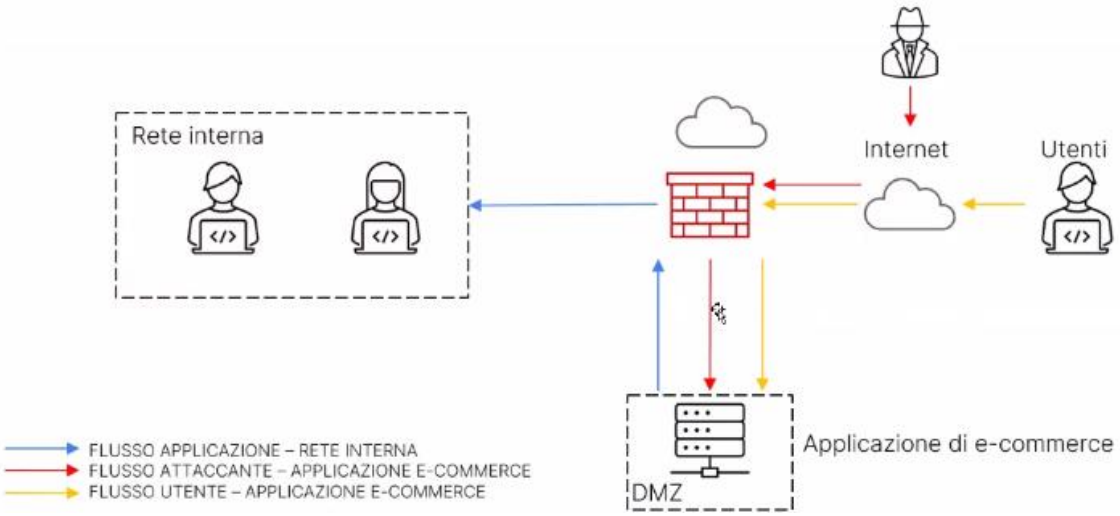
3. Response: l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostra rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificare la figura sotto con la soluzione proposta

4. Soluzione completa: unire i disegni dell'azione preventiva e della response

5. Modifica "più aggressiva" dell'infrastruttura (se necessario/facoltativo magari integrando la soluzione al punto 2)

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.

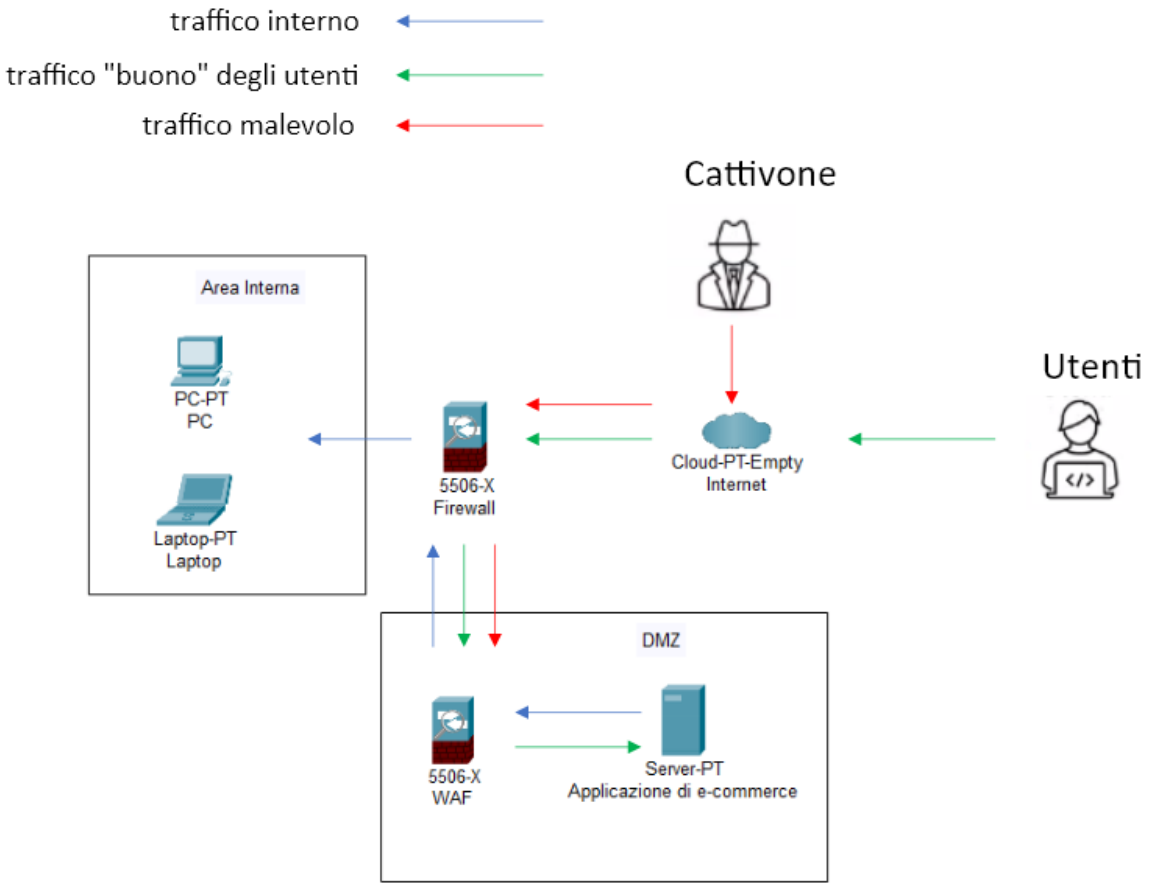


Soluzioni

1.

Per difendere l'applicazione Web da attacchi di tipo SQL/XSS da parte di un attaccante esterno possiamo ricorrere all'utilizzo di un WAF (Web Application Firewall).

Il WAF analizza il traffico in entrata, filtrando il traffico e bloccando quello malevolo, e in uscita, impedendo la diffusione di dati non autorizzati dall'applicazione, dalle applicazioni Web.



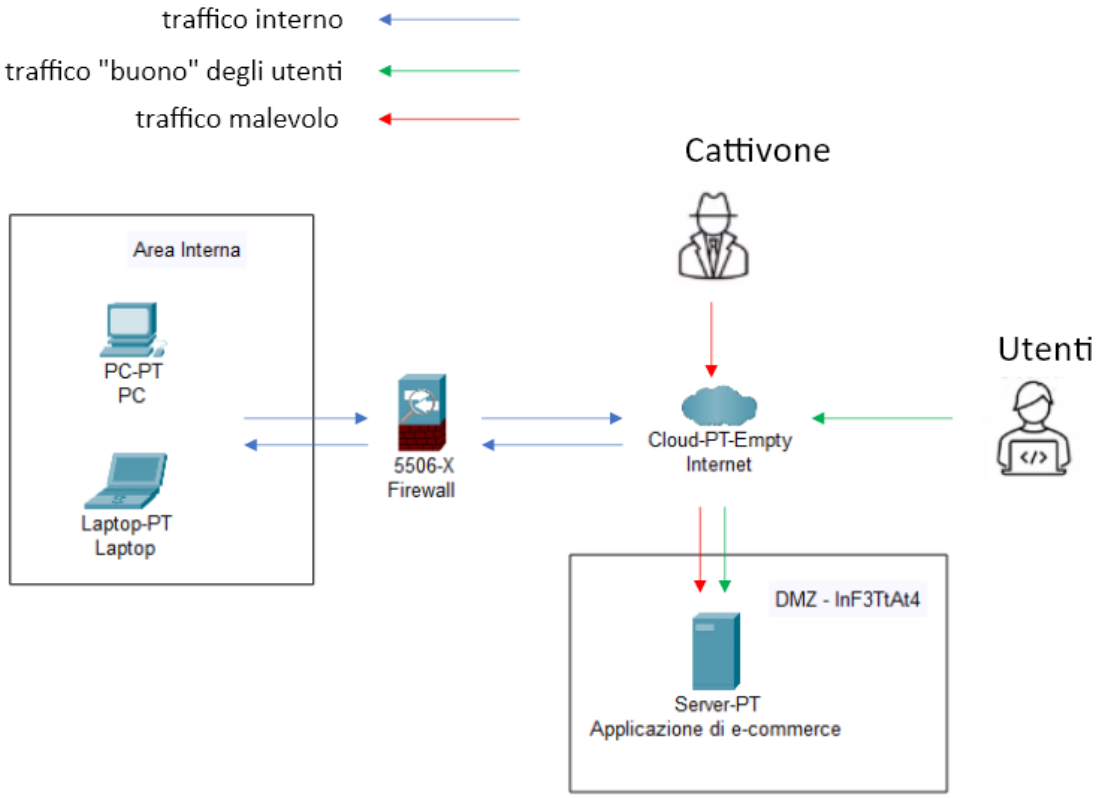
2.

Considerando una perdita di €1 500 per minuto di inattività del servizio, a seguito di un attacco DdoS che rende indisponibile il servizio per 10 minuti, si raggiungerebbe una perdita approssimativa uguale a €15 000.

Delle azioni preventive contro gli attacchi DDoS potrebbero essere: l'utilizzo di un WAF (consigliato già nella soluzione 1), efficaci contro questi tipi di attacchi grazie alla loro abilità di individuare il traffico malevolo; l'utilizzo di quello che viene chiamato DraaS, Disaster Recovery as a Service, con questo metodo i cloud provider offrono un?infrastruttura in cloud che si attiva immediatamente quando il sito primario della compagnia non riesce ad erogare i propri servizi per qualsiasi incidente. Vantaggi di questo servizio sono il costo basso, viene pagato solo per tempo di utilizzo, e la tempestività di intervento per quanto riguarda la continuazione del business mentre, tra gli svantaggi, abbiamo una maggiore latenza dovuta allo "switch" da sito primario a sito secondario.

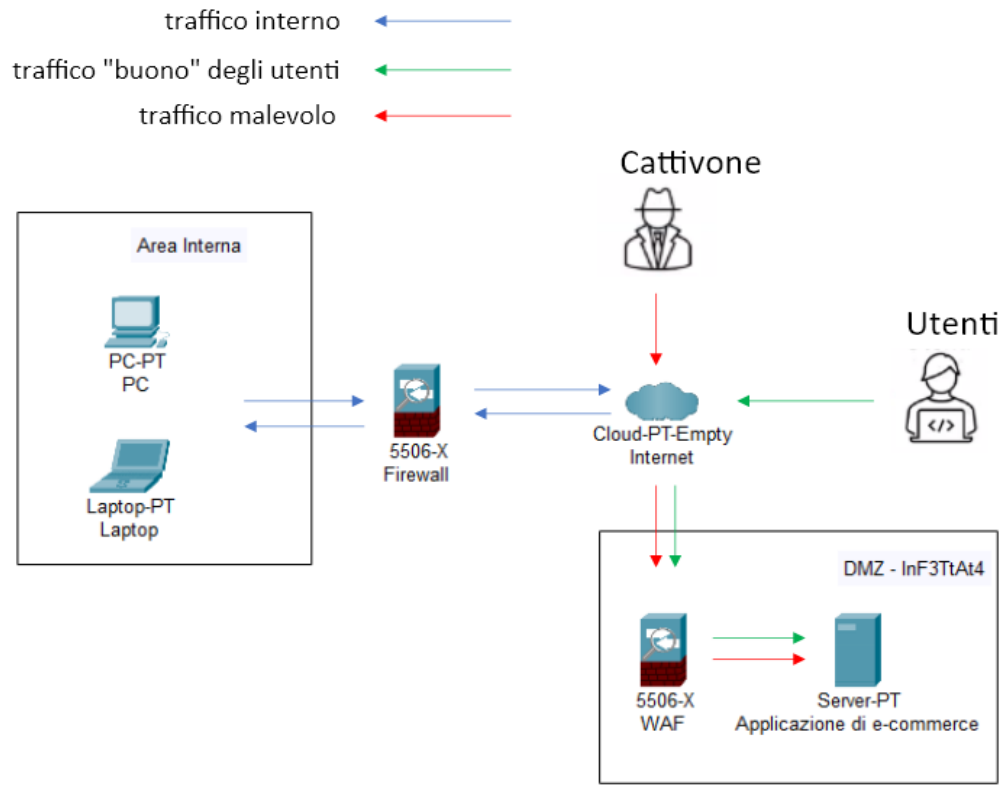
3.

A seguito di un malware che è riuscito a infettare l'applicazione Web, al fine di salvaguardare la sicurezza della rete interna, applichiamo un'approccio di isolamento del sistema infetto: l'applicazione Web infetta resterà raggiungibile dall'attaccante che però non avrà modo di accedere alla rete interna, questo approccio permetterà di studiare il comportamento dell'attaccante senza rischiare di compromettere la sicurezza interna.



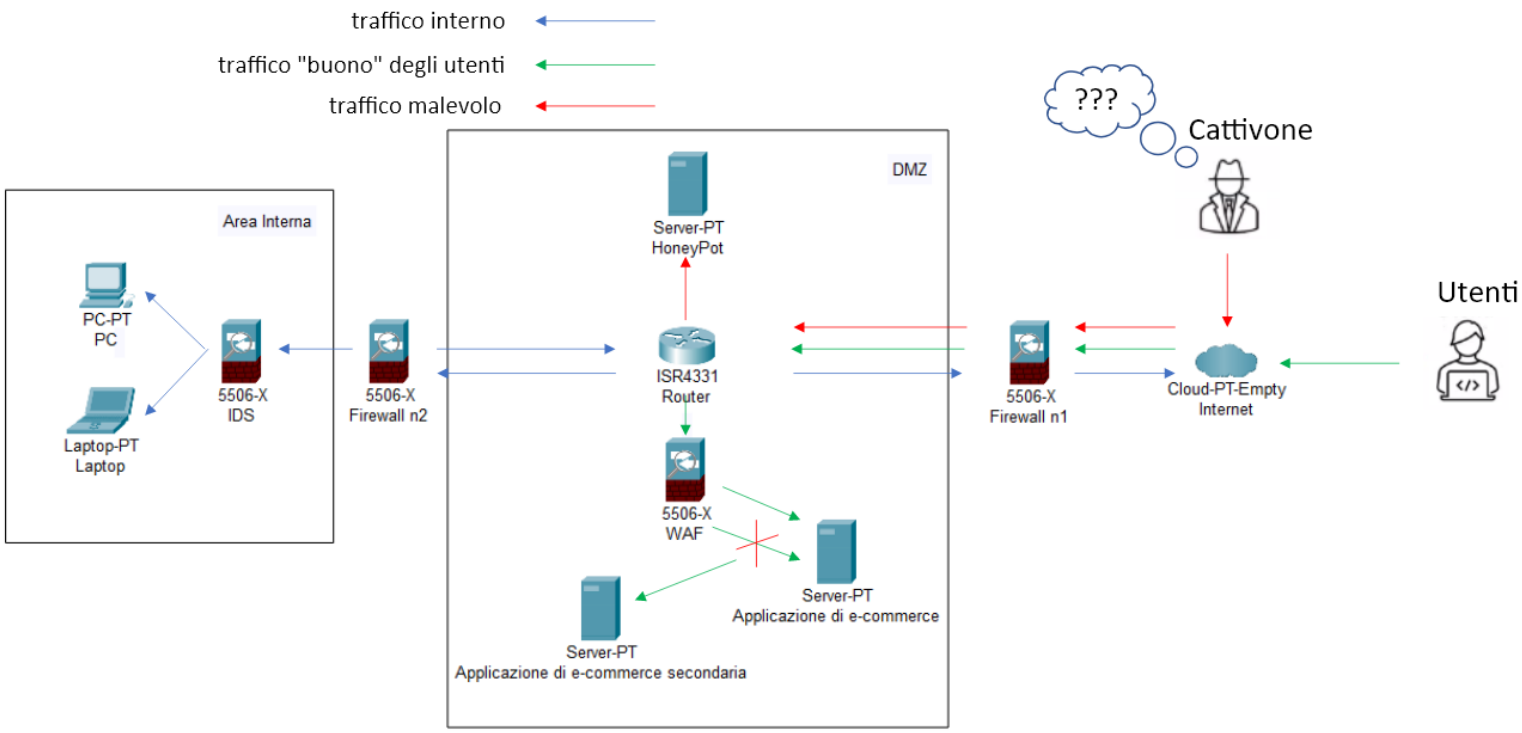
4.

Disegno risultato dall'unione delle soluzioni 1 e 3.



5.

Qualora si volesse procedere con una “ristrutturazione” dell’infrastruttura di una certa importanza propongo una modifica di questo tipo:



HoneyPot: svolge la funzione di specchietto per le allodole, attira i malintenzionati che cercano di entrare con la forza sfruttando delle vulnerabilità del sistema in un ambiente dove non possono causare danni.

IDS: è un sistema di rilevamento delle intrusioni che informa in caso di accesso non autorizzato.

Applicazione secondaria: se a causa non per forza dell’attacco di un malintenzionato dall’esterno, ma anche solo un guasto dovuto a usure/difetto di funzionamento dell’applicazione Web il servizio rimarrebbe indisponibile, penso sia saggio valutare l’introduzione di un sistema ausiliario che intervenga in aiuto del primario in caso di incidenti. Questo sistema secondario può essere pensato sia fisicamente con hardware, software e risorse pronte all’utilizzo o anche in cloud con servizi come il RDaaS spiegato precedentemente nella soluzione 2.

Firewall aggiuntivo: si consiglia l’aggiunta di un secondo Firewall DIVERSO dal precedente, se il primo presenterà una vulnerabilità data dalle proprie configurazioni di fabbrica (bug, vulnerabilità 0-day) le probabilità che lo stesso problema si ripercuotano sul secondo Firewall di diversa tipologia si riducono notevolmente, assicurando la protezione dell’area interna in caso di “caduta” del primo Firewall.