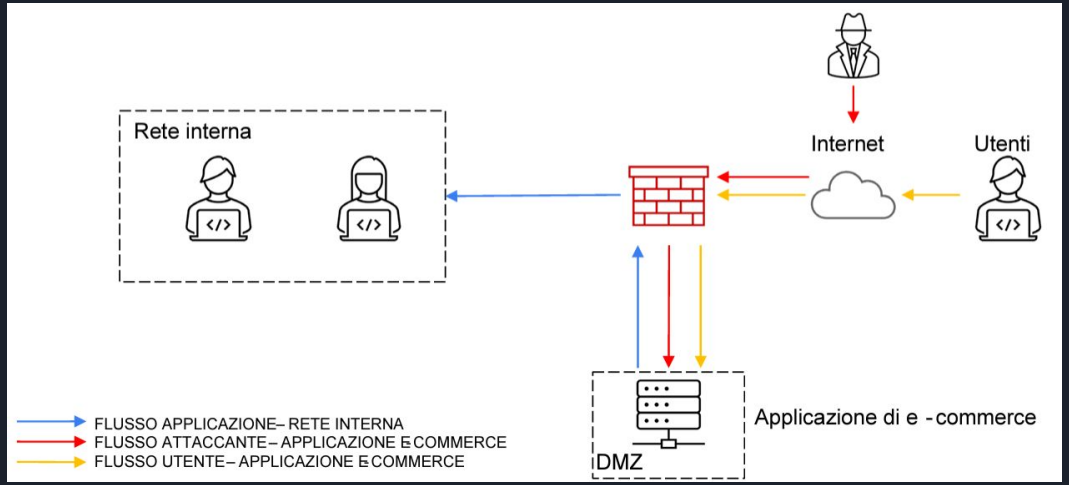
PROGETTOS9/L5

INTRODUZIONE

Nell’esercizio di oggi ci vengono fatte richieste multiple che saranno divise in cinque punti:

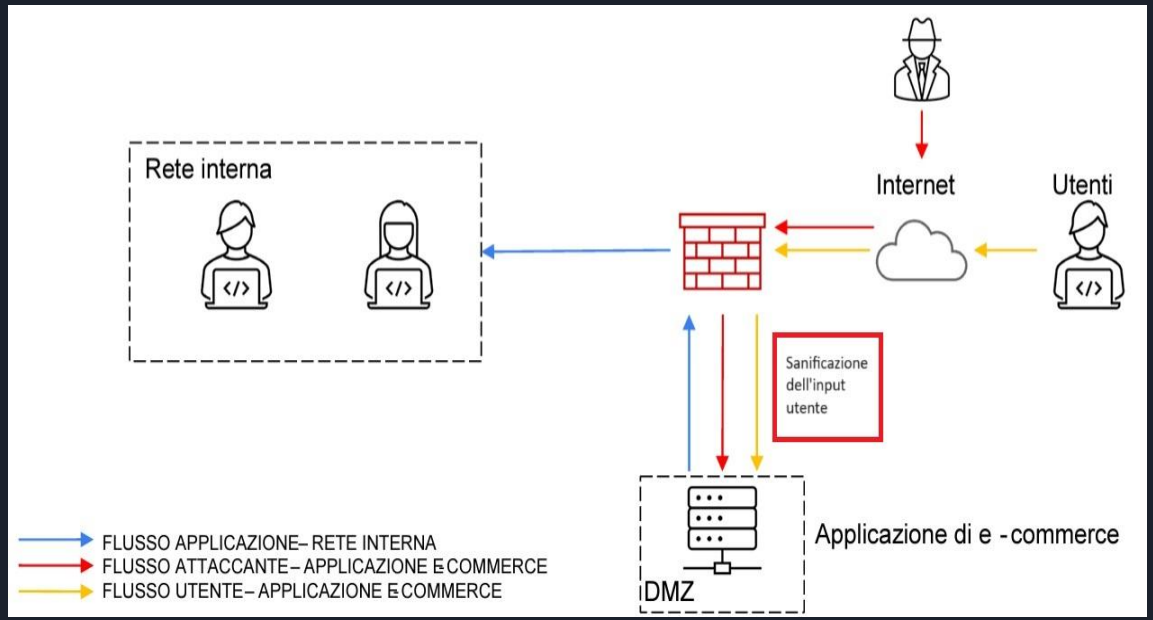
1) Azioni preventive;
2) Impatti sul business;
3) Response;
4) Soluzione completa;
5) Modifiche aggiuntive.

Faremo riferimento alla figura accanto per rispondere ai quesiti dell'esercizio. L'applicazione di e-commerce nella DMZ, usata dagli utenti per fare acquisti, deve essere raggiungibile da internet. La rete interna è raggiungibile dalla DMZ per via delle regole impostate sul firewall, quindi potenzialmente attaccabile se il server viene compromesso.



Traccia 1: Azioni Preventive

Nella traccia ci viene chiesto di eseguire azione preventive per evitare un possibile attacco XSS o SQL injection. Queste sono vulnerabilità date dal codice di programmazione che accetta un input dall'utente senza validarlo. Per risolvere questa vulnerabilità basta sanificare l'input.



Traccia 2: Impatti sul business

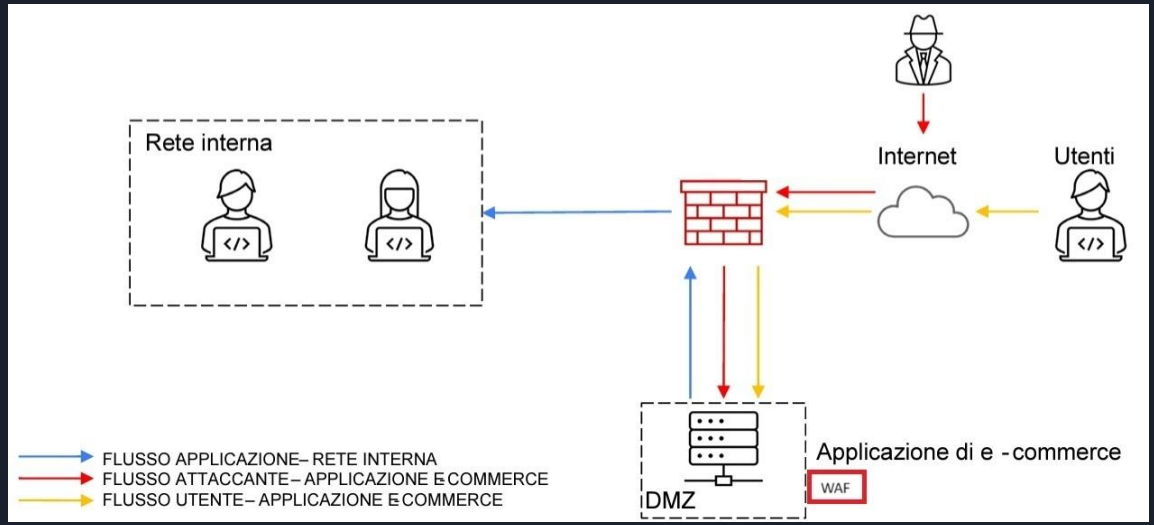
Nella traccia viene presentato uno scenario in cui il sito di e-commerce subisce un attacco DDOS e va in down per 10 min. Ci viene chiesto di calcolare l'impatto sul business e suggerire eventuali azioni preventive da applicare.

In media vengono spesi 1500€ al minuto sulla piattaforma per cui basta eseguire il prodotto tra questo dato e il tempo in cui il sito non è raggiungibile:

Perdita media = 1.500€ * 10 min = 15.000€

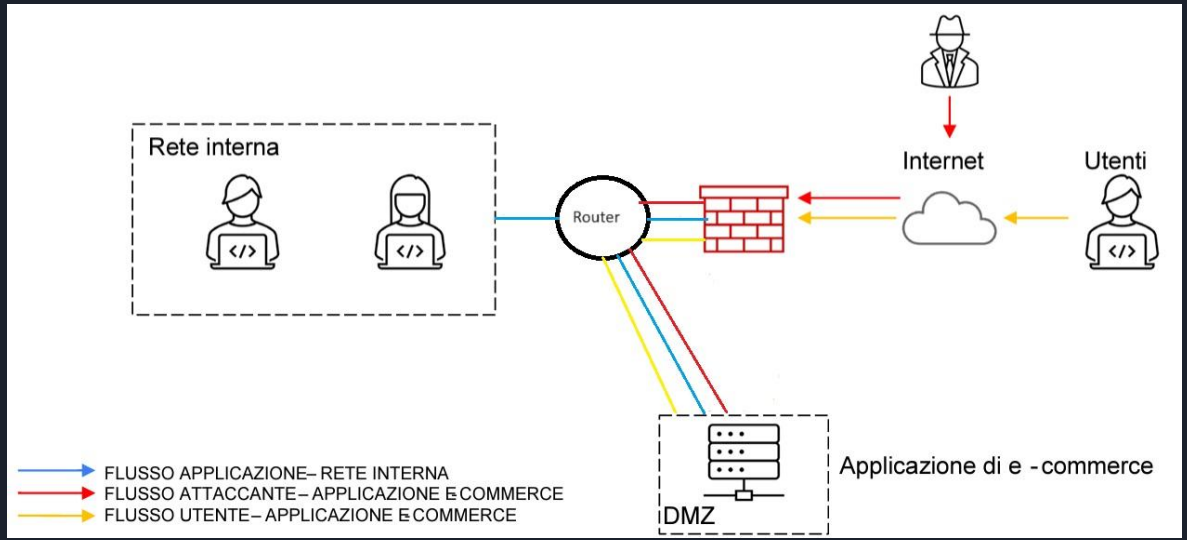
Ci sono diverse misure preventive che si possono applicare in un caso come questo. Ovviamente bisogna essere sempre preparati ad ogni evenienza, quindi è buona norma mantenere tutti i dispositivi e le applicazioni aggiornati e creare dei piani di incident response. Oltre a questo si può intervenire sui TTL riducendoli per le richieste in attesa oppure implementando soluzioni di sicurezza, hardware o software, aggiuntive.

Per esempio si può implementare un WAF sul sito di e-commerce. Questo è uno strumento software che va a proteggere l'applicazione a cui è associato filtrando il traffico http.



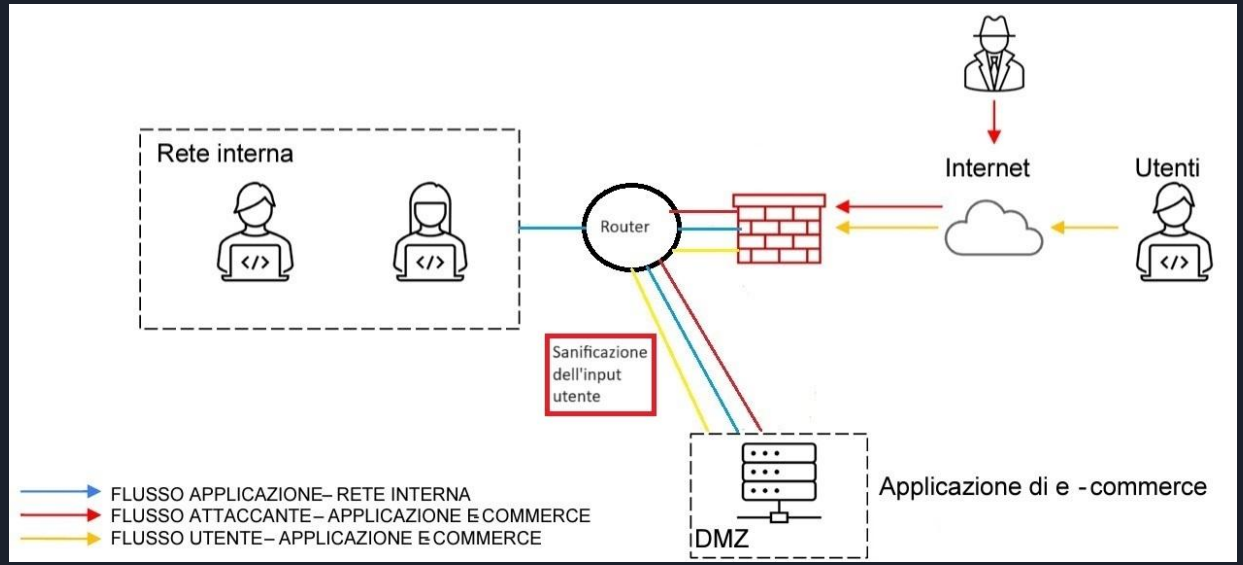
Traccia 3: Response

Ci viene presentato lo scenario di un attacco malware all'applicazione web. La nostra priorità è bloccare la diffusione dell'attacco. Possiamo implementare un router, come in figura, e configurarlo in modo da tenere la DMZ e la intranet separate su due reti diverse. In questo modo il malware non sarà in grado di raggiungere la intranet.



Traccia 4: Soluzione completa

Nella quarta traccia ci viene chiesto di unire le soluzioni della terza e della prima traccia in modo da avere tutto su un'unica rete.



Traccia 5: Modifiche aggiuntive

La traccia ci chiede di effettuare modifiche aggiuntive alla rete per migliorarne la sicurezza. Ipotizzando di avere ulteriore budget a disposizione possiamo pensare all'implementazione di un IPS basato sull'analisi delle anomalie. Questo strumento ci consente di conoscere la nostra rete e di monitorarne il traffico. Esso prevede una iniziale raccolta di statistiche della rete per capire come si presenta il traffico in condizioni normali. Confrontando le statistiche attuali con quelle registrate sarà in grado di bloccare eventuali anomalie. Possiamo inoltre integrare la soluzione della seconda traccia.