Traccia:

Con riferimento alla figura in slide 2, rispondere ai seguenti quesiti.

1. **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?
   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**

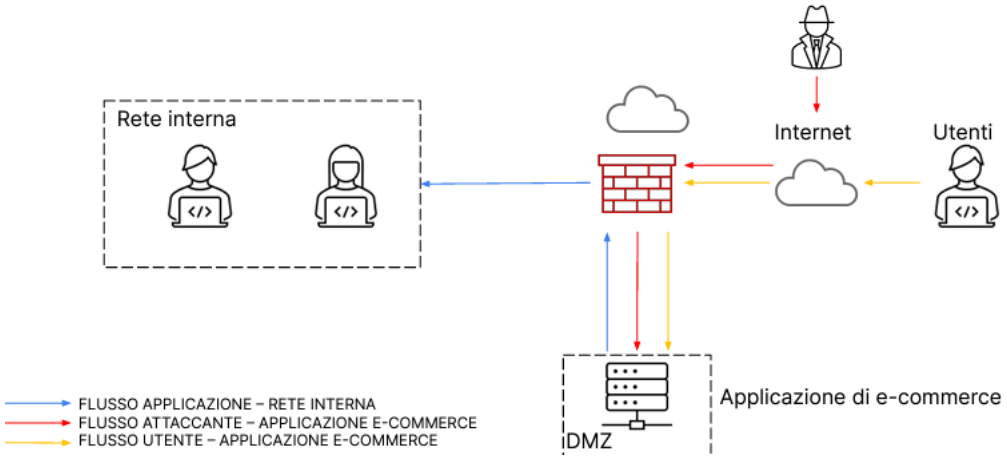
3. **Response**: l'applicazione Web viene infettata da un malware.
   La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata.
   Modificate la figura in slide 2 con la soluzione proposta.

4. **Soluzione completa**: unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)

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

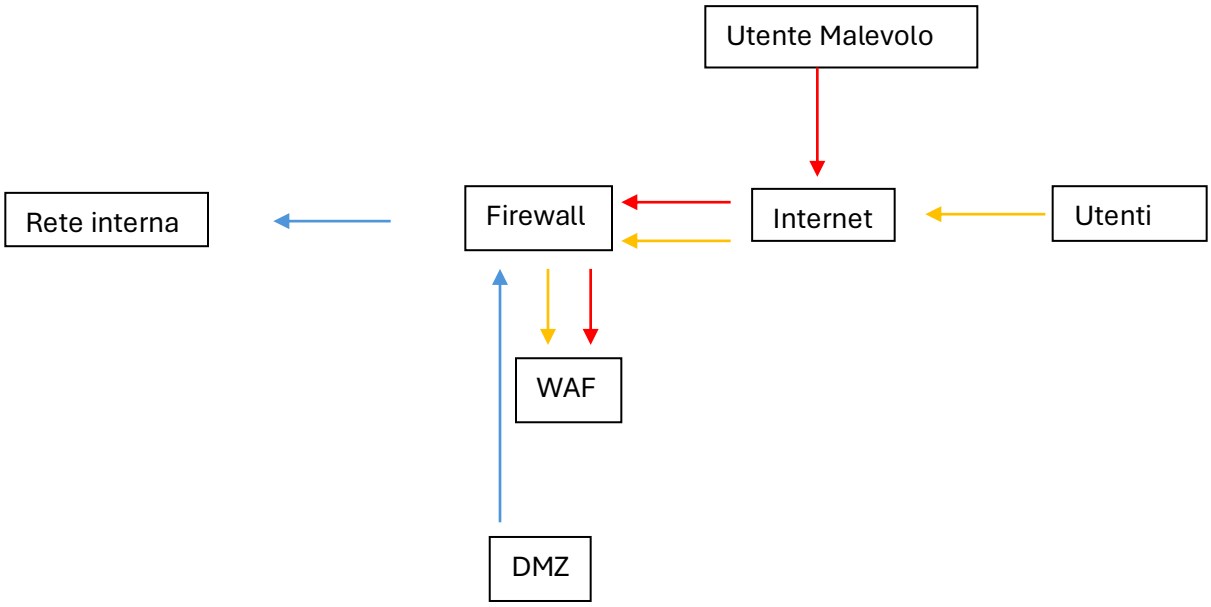
Architettura di rete:
L'applicazione di e-commerce deve essere disponibile per gli utenti tramite Internet per effettuare acquisti sulla piattaforma.

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.



1. Una serie di misure preventive da implementare per difendere una Web App possono essere implementate dopo aver effettuato una Vulnerability Assessment per identificarne le vulnerabilità e un successivo Penetration Testing per identificare e risolvere delle criticità. Nel caso che un utente malintenzionato decida di effettuare attacchi SQLi o XSS potrebbe sicuramente essere fare una SDLC, un processo economico ed efficiente in termini di tempo che i team di sviluppo utilizzano per progettare software di qualità. L'obiettivo del SDLC è quello di ridurre al minimo i rischi del progetto attraverso la pianificazione preventiva, in modo che il prodotto soddisfi le aspettative dei clienti. Altri elementi da installare sarebbero i Web Appllication Firewall (WAF), i quali sono dei dispositivi di sicurezza dediti alla protezione delle applicazioni Web da attacchi dannosi e traffico indesiderato inclusi bot, injection e denial of service (DoS) a livello di applicazione. Il WAF permetterà di definire e di gestire le regole per evitare minacce da internet raccogliendone i log di accesso per la

conformità delle analisi. Infine, risulta necessario inserire un protocollo di test periodici per monitorare la situazione dell'applicazione.



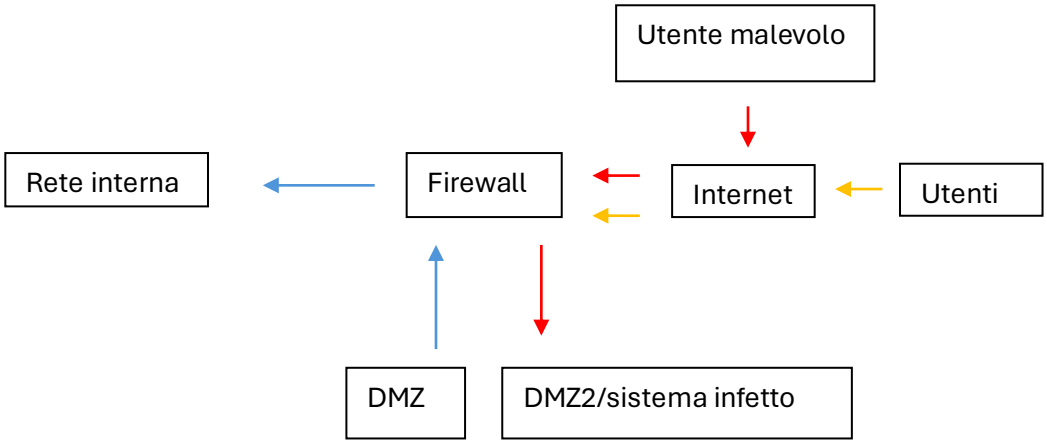
2. Per calcolare l'impatto che l'attacco DDoS ha avuto, rendendo irraggiungibile l'applicazione di e-commerce, è possibile ipotizzarlo mediante alcuni scenari. Bisogna intanto capire se questo tipo di attacco si può manifestare una volta l'anno, una volta al mese o risulta essere un problema giornaliero, ognuno di questi casi può presentare una differente tipologia d'impatto per la piattaforma. Fra le azioni preventive da implementare durante il BCP risulta necessario, in questo caso, calcolare anche il costo di un software anti DDoS, per poter ridurre la possibilità di un attacco analogo che possa nuocere nuovamente all'azienda analizzando l'architettura di rete, individuando gli spazi e aree di gestione indispensabili evidenziando i servizi critici dell'azienda e riflettendo che tipo di protezione adottare. La scelta di una soluzione di questo genere deve venire valutata in base al tipo di azienda attaccata tenendo in considerazione un'eventuale accettazione del rischio; nel caso proposto dal quesito il rischio si presenterebbe alto se un attacco simile dovesse perpetrare per 24h, a valle del problema deve essere inserito nel BCP anche il costo di un'adeguata protezione DDoS.

   Ipotizzando alcuni scenari se l'attacco avvenisse quotidianamente per 10 minuti per un anno, la compagnia in questione avrebbe un danno di circa 129.600.000€, in questo caso sarebbe indispensabile pensare ad un'azione preventiva. Potrebbero venir messe sul tavolo una serie di soluzioni con costi e servizi offerti in base alle necessità dell'azienda. Ipotizzando un costo di 1000€/mese, in base alle necessità, per l'acquisto di un sistema di protezione adeguato, potrebbe rivelarsi una spesa sopportabile per l'integrità aziendale.

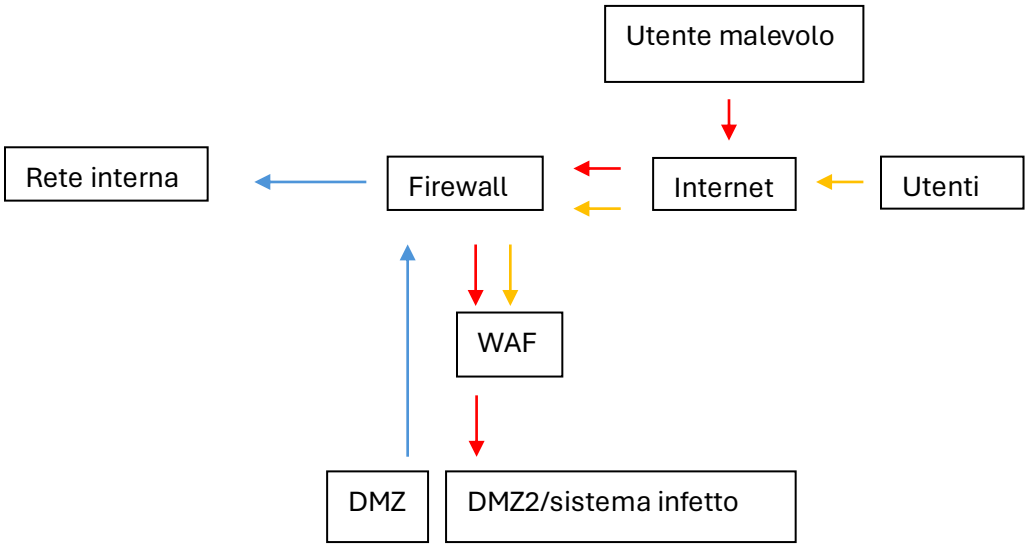
   Se l'attacco dovesse invece manifestarsi una volta il mese, sempre per la durata di 10 minuti il danno sarebbe di 180.000€/anno e anche in questo caso la stessa spesa di 1000€/mese continuerebbe ad essere piuttosto conveniente per far fronte alla minaccia DDoS, ma non sono da escludere eventuali piani con tariffe più basse.

   Se l'attacco venisse effettuato un'unica volta per anno la perdita sarebbe significativamente bassa e non è da escludere che un'azione preventiva anti DDoS si riveli avere un costo più elevato rispetto a lasciar verificare l'attacco e spendere una cifra di 1000 o 500€/mese potrebbe non essere economicamente accettabile per l'azienda.

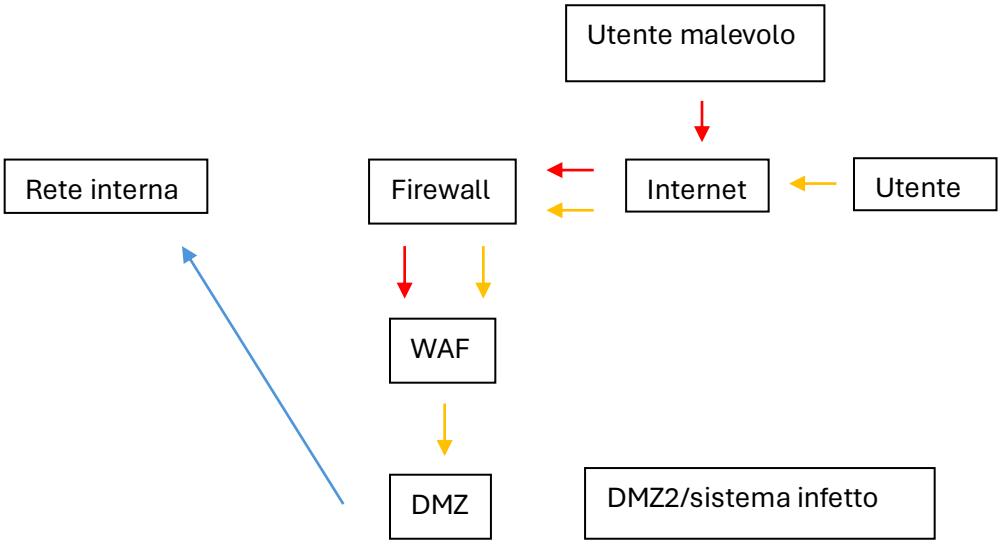
3. Nel caso di un sistema infettato da un malware è necessario attuare delle azioni correttive partendo da una segmentazione della rete aziendale oltre che configurare delle policy firewall ad hoc per la protezione del sistema e monitorando gli accessi degli utenti mediante la raccolta di log. Un'ulteriore azione da attuare riguarda sicuramente l'isolamento del server compromesso in un nuovo segmento di rete per poter procedere con la rimozione del problema senza rischiare di infettare altri elementi del sistema. La rete interna risulta dunque raggiungibile dalla DMZ a causa delle policy sul firewall, se la DMZ viene compromessa allora un utente malevolo può raggiungere la rete interna.



4. Soluzione finale.



5.



Un’azione più aggressiva e drastica da poter adottare potrebbe essere la rimozione dell’elemento DMZ2 infetto dall’architettura generale e cambiare il sistema di gestione dei contenuti (CMS) della piattaforma e-commerce.