Progetto Modulo 5 :

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 dalla non raggiungibilità del servizio, considerando che in media ogni minuto gli utenti spendono 1500€ 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'accessa 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)

Svolgimento :

Punto n°1 :

Per prevenire attacchi di tipo SQLi e XSS da parte di un malintenzionato , si deve predisporre l'applicazione web in modo tale da accettare in input solo un input sanificato, quindi devono essere predisposti controlli di convalida dell'input impedendo di usare caratteri speciali ad esempio, che vengono generalmente usati per exploitare le ricerche all'interno dei database. Inoltre bisogna mantenere sempre aggiornata l'infrastruttura con patch mirate atte a rimediare le vulnerabilità note dei sistemi in uso sulla web app.

Punto n°2 :

Nel caso in cui un attacco DDoS renda la web app non raggiungibile per 10 minuti dobbiamo calcolare l'impatto sul business.La cifra si aggirerà mediamente sui 15 K euro.
Per difendere l'applicazione web da un attacco di tipo DDoS potremmo ricorrere a due diverse soluzione :

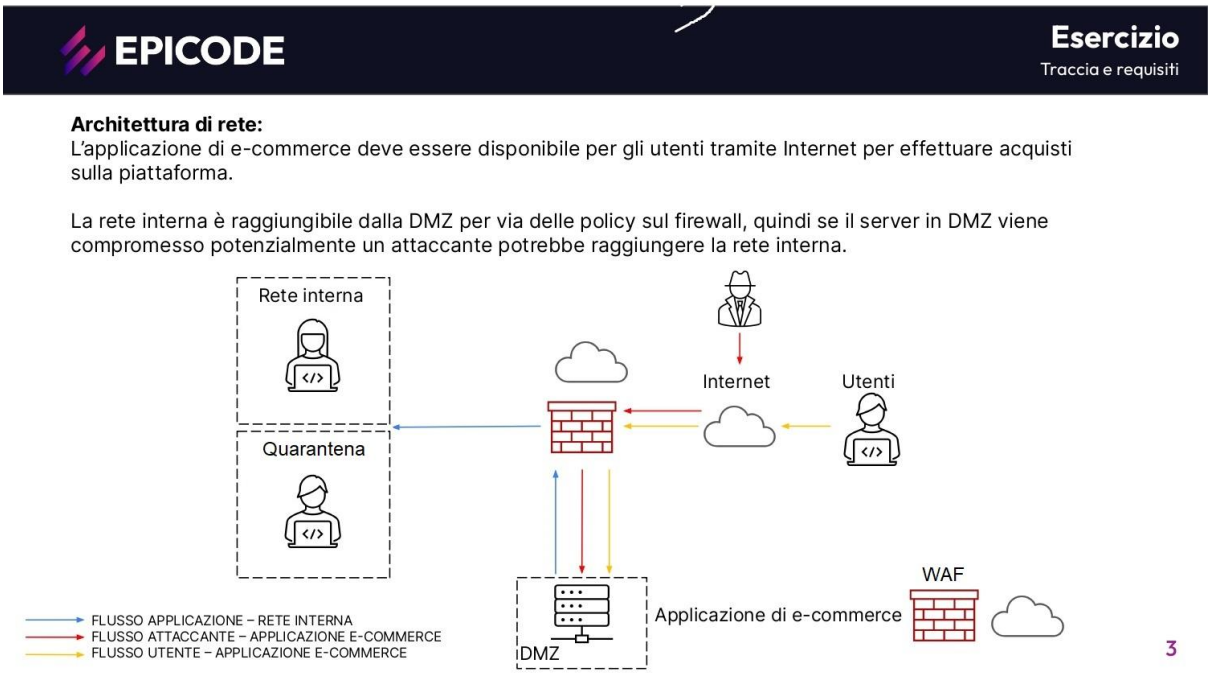
1. sicuramente modificare le regole presenti sul firewall, impedendo al server presente sulla DMZ di accedere alla rete interna. Inserendo infatti una regola che vieta il traffico dall'ip del server a tutta la subnet della rete interna possiamo impedire in maniera gratuita e immediata la possibilità di attacchi una volta che il server presente nella DMZ viene compromesso.
2. un'altra soluzione , ovviamente più costosa in quanto quella suggerita nel punto precedente è gratuita, è quella di comprare un WAF e metterlo tra internet e la DMZ così da proteggere il server da attacchi web provenienti da Internet.
3. Nel caso si disponga della disponibilità economica necessaria si può pensare all'implementazione di un cluster di server ridondanti. Avendo infatti una coppia di server sulla quale bilanciare il traffico proveniente dall'esterno andiamo a limitare la possibilità di avere un Single Point of Failure.
4. Ovviamente la soluzione ideale prevederebbe l'uso del cluster e del WAF in contemporanea, ma resta da capire se l'azienda ha la disponibilità economica per sostenere la spesa.

Punto n°3 :

Per evitare che il malware si propaghi su tutta la rete del dispositivo infettato, possiamo procedere in due maniere.
Isolazione del dispositivo infetto, o segmentazione della rete.
Nell'isolazione del dispositivo si va a disconnettere l'apparato infetto dalla rete, limitando così l'accesso a internet del dispositivo, impedendo quindi al threat actor di continuare a mantenerne il possesso.
Visto che però non è questa la richiesta, si può segmentare la rete, spostando il dispositivo in una rete di quarantena creata appositamente per evitare che il malware si propaghi nella rete del dispositivo infetto.

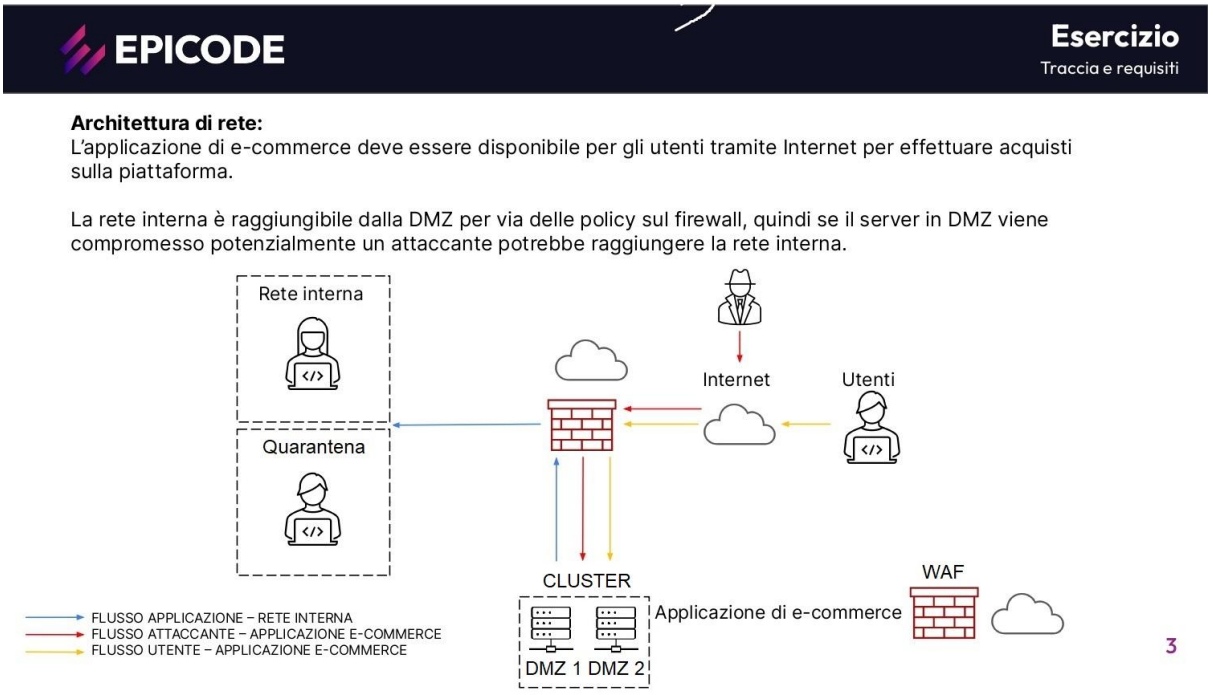
Punto 4 :

Come detto in precedenza, le modifiche implementate risulterebbero così :



Punto 5 :

Implementando tutte le modifiche da me suggerite l'infrastruttura risulterebbe la seguente :



E' stato creato un cluster dei server che per l'esempio ho chiamato solo a scopo illustrativo DMZ 1 e DMZ2, il pc dell'utente infetto è stato messo in quarantena, e come possiamo vedere è stato installato un WAF tra internet e il CLUSTER dei server nella zona demilitarizzata.