Gabriele Di giampietro **Progetto Settimanale 23/12/2022**

Obbiettivo: In riferimento alla rete nell'immagine fornita, proporre le seguenti soluzioni:

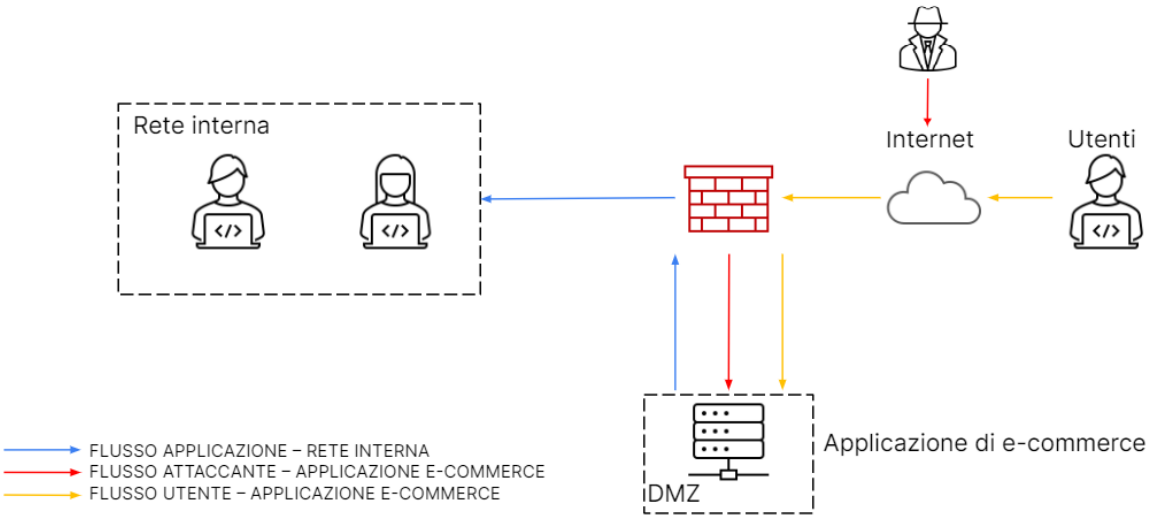
- **Azioni Preventive: implementare delle azioni preventive per difendere la Web application da attacchi di tipo SQL e XSS, modificando la rete fornita.**

- **Calcolare l'impatto del business dovuto alla non raggiungibilità del servizio, considerando che in media gli utenti spendano 1.500 € sulla piattaforma e-commerce, causata da un attacco Ddos che rende l'applicazione non raggiungibile per 10 minuti.**

- **Response: Avviare una tecnica di response perché la Web application è stata infetta da Malware. La vostra priorità è che il Malware non si propaghi nella rete interna, senza preoccuparsi che l'attaccate abbia ancora accesso alla Web app, modificando la rete fornita.**

- **Soluzione completa: Unire modificando la rete fornita la soluzione preventiva e quella del response.**

- **Bonus: Modifica la rete in modo più aggressivo la rete, se necessario.**



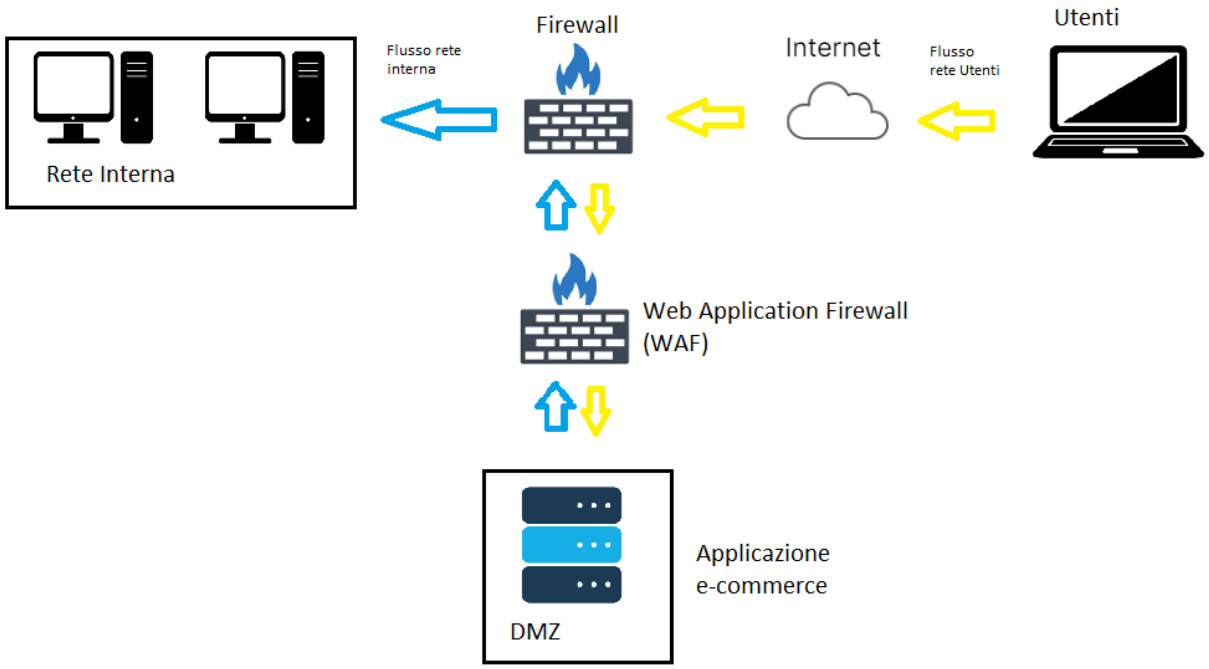
Azioni Preventive

La prima soluzione che andiamo a proporre è la modifica della nostra rete fornita nella task, cercando di prevenire un attacco alla nostra **Web application** che nel nostro caso è un **sito di e-commerce.**

In questa prima casistica non inseriamo l'attaccante perché ci troviamo in una **fase di prevenzione** e quindi il nostro scopo è quello di cercare di evitare l'attacco, proteggendo al meglio il nostro sito di e-commerce che si trova in una **DMZ (Area demilitarizzata)** priva di protezioni elevate proprio per fare accedere gli utenti che intendo fare acquisti sul sito. Una soluzione che possiamo apportare è l'inserimento, sulla linea che va alla Web app, di un **Web application Firewall (WAF)**: I Web Application Firewall (WAF) consentono di **proteggere le applicazioni Web da attacchi dannosi** e

traffico Internet indesiderato, inclusi bot, injection e denial of service (DoS) a livello di applicazione. **Il WAF consentirà di definire e gestire le regole per evitare minacce** a Internet, tra cui indirizzi IP, intestazioni HTTP, corpo HTTP, **scripting (XSS), inserimento SQL** e altre vulnerabilità. Il firewall dell'applicazione Web viene distribuito per proteggere le applicazioni Web e raccogliere i log di accesso per la conformità e l'analisi.

Le frecce di colore azzurro indica il flusso della rete interna che comunica con la Web application, mentre le frecce di colore giallo indicano il flusso degli utenti che accendo sempre alla Web application e cioè al sito di e-commerce.



Impatto del Business

In questo caso dobbiamo invece ipotizzare che il nostro sito di e-commerce sia fuori servizio a causo di un attacco Ddos sulla nostra web application. Supponendo che gli utenti spendano 1.500 € al minuto e che il servizio non è disponibile per 10 minuti, dobbiamo calcolare l'impatto economico dell'attacco.

Possiamo fare un semplice calcolo con cui chiameremo la **spesa media degli utenti (SU)** e il **tempo in cui il nostro sito è fuori servizio (T).** Moltiplichiamo la mancata spesa degli utenti per il tempo di disservizio. Quindi avremo la seguente formula:

Impatto del Business=SU*T= 1500*10= 15000

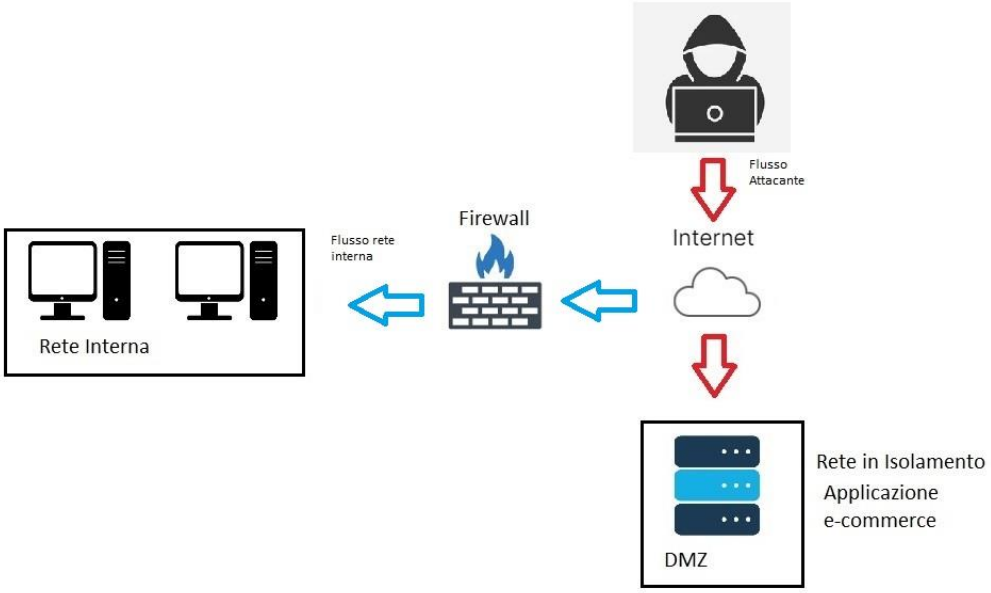
Possiamo quindi dire che l'attacco Ddos sul nostro sito di e-commerce durato 10 minuti ci da un Impatto del business di 15000 €.

Response

Adesso ci occuperemo invece di una Response sapendo che **la nostra applicazione Web è stata attaccata ed è infettata da un Malware**. Dobbiamo quindi **proteggere la nostra rete interna** perché sappiamo che essendo in comunicazione con la Web app, da quest'ultima il Malware potrebbe accedere alla rete interna che contiene dati sensibili e altre sistemi importanti.

Uno dei metodi migliori per prevenire e proteggere le reti è quello della **segmentazione**, ma può non bastare perché comunque l'attaccante può risalire dalle altre reti segmentate fino a quella interna. Però nel nostro caso possiamo usare **la tecnica dell'isolamento**, cioè **isolare il sistema compromesso** dalla rete interna così da **limitare l'attacco alla sola Web application**: l'attaccante continuerà ad avere la possibilità di attaccare, ma non potrà accedere alla rete interna perché non più in comunicazione con l'applicazione Web compromessa.

Le frecce azzurre indicano il flusso della rete interna (collegata solamente ad internet in senso generico) che come vediamo non riceve più comunicazione dall'applicazione e-commerce, essendo una **rete in isolamento o di quarantena**. Mentre le frecce rosse indicano il flusso dell'attaccante che continua ad avere accesso all'applicazione Web, ma che non potrà raggiungere da essa la rete interna.

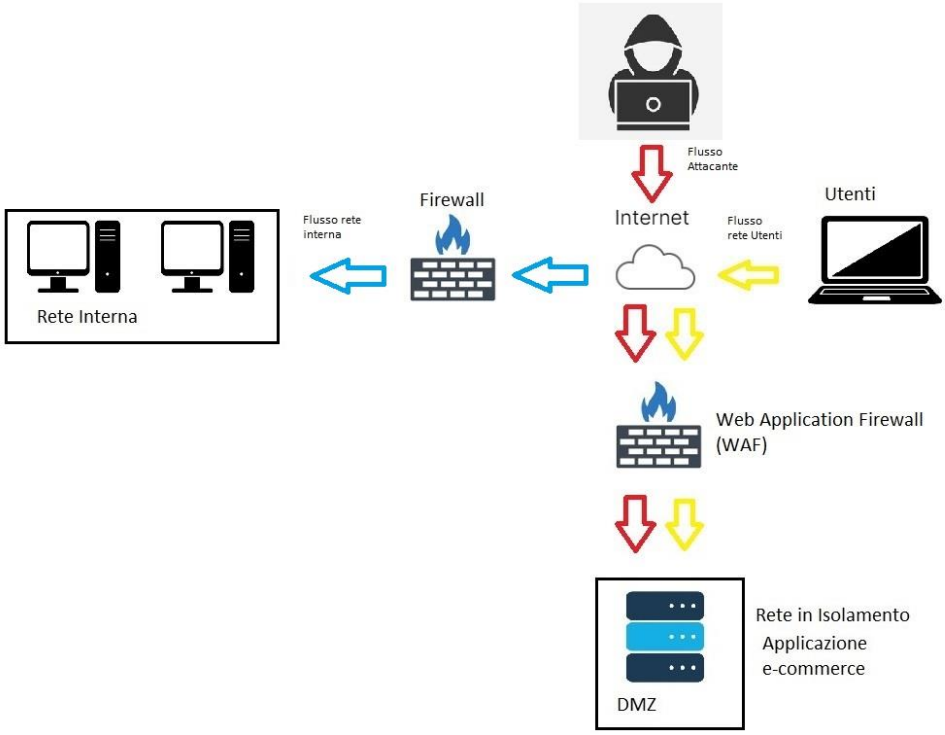


Soluzione Completa

Per avere un quadro completo delle situazioni che abbiamo affrontato in questa esercitazione, **uniamo la soluzione dell'azione preventiva e quella del response in unico schema di rete**. Mostrando così come la rete che proponiamo possa prevenire e proteggersi in caso di attacco, mantenendo però la Web application attiva, limitando i danni sia tecnici che economici all'azienda e ai sui utenti.

Le frecce azzurre indicano sempre il flusso della rete interna che rimane separata dall'applicazione dell'e-commerce che lasceremo in isolamento, in quanto c'è la possibilità che sia ancora compromessa. Le frecce rosse sono il flusso dell'attaccante, che in questo caso potrebbe ancora

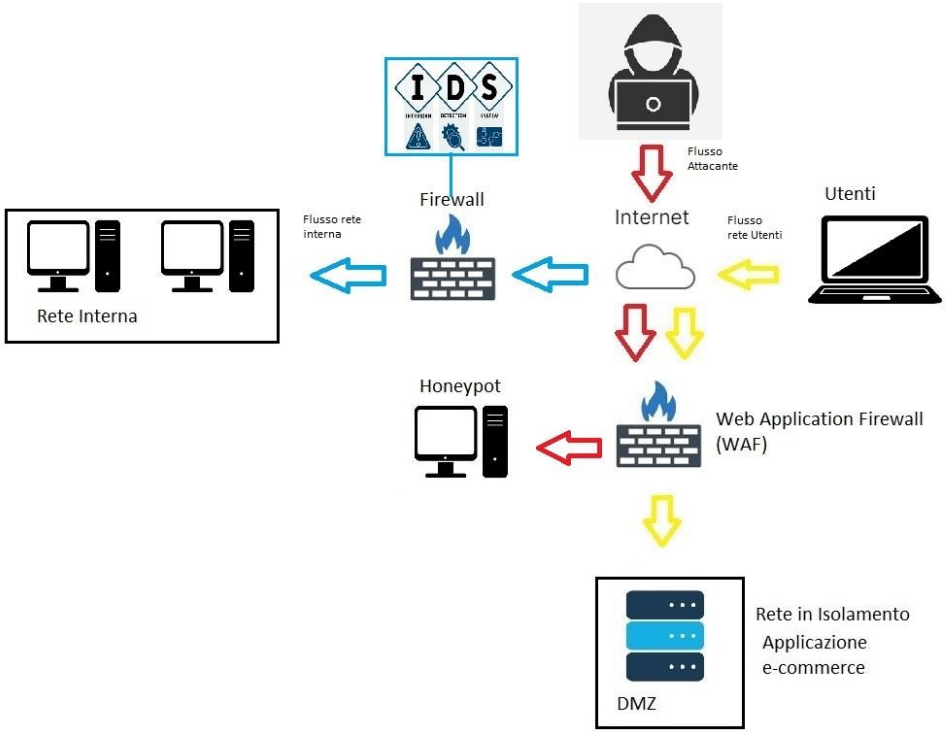
attaccare la Web app, mentre quelle gialle degli utenti che accedono al sito di e-commerce. Abbiamo lasciato il WAF che funge da protezione per la Web application e per gli utenti che possono esser vittime di uno script XSS o di uno SQL injection (ad esempio il furto dei dati riservati degli utenti registrati nel sito e-commerce). Con questa soluzione l'azienda potrebbe limitare i danni non chiudendo il servizio del sito e-commerce fino a che non attiverà una nuova applicazione web su cui trasferirsi (come per esempio un Cold site) non compromesso o ricostruire da capo il sistema compromesso.



Bonus

In questa ultima soluzione, abbiamo ipotizzato, basandoci sempre dalla stessa rete proposta un'infrastruttura più protetta e controllata.

Abbiamo lasciato sempre la nostra Web application in isolamento, in quanto potrebbe essere compromessa e se la situazione lo rende necessario può essere anche rimossa sia dalla comunicazione con la rete interna sia da internet, questa strada bloccherebbe totalmente l'attaccante ma non permetterebbe più l'accesso neanche agli utenti. Poi abbiamo aggiunto un **honeypot** per trarre in inganno l'attaccante e indirizzarlo su una scatola vuota, infine abbiamo anche aggiunto **IDS** in parallelo al Firewall della rete interna così da monitorare le attività sospette inviate ad un **SOC** (Security Operation Center) o gestite da un **SIEM** (Security Information and Event Mangement) per esempio.


I D S
Flusso
Attacante
Firewall
Internet
Utenti
Flusso rete
interna
Flusso
rete Utenti
Rete Interna
Honeypot
Web Application Firewall
(WAF)
Rete in Isolamento
Applicazione
e-commerce
DMZ