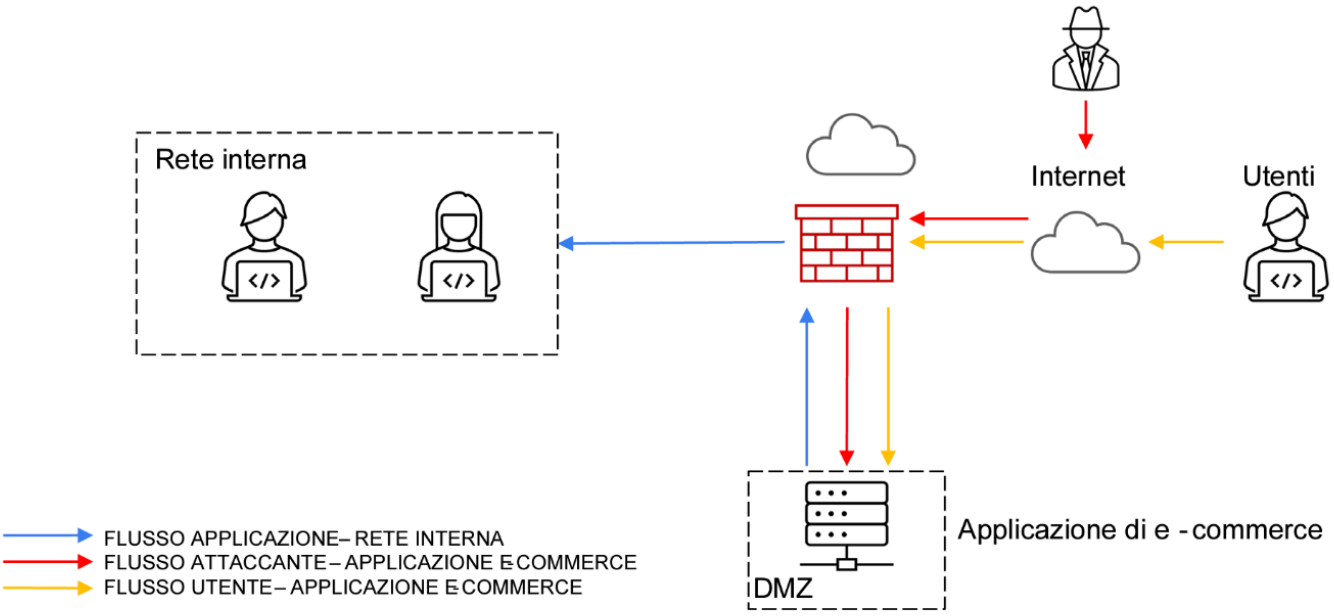
Progetto S9/L5

Stefano Di Prospero

Traccia:

1. Azioni preventive
2. Impatti sul business
3. Response
4. Soluzione completa
5. Modifica più aggressiva



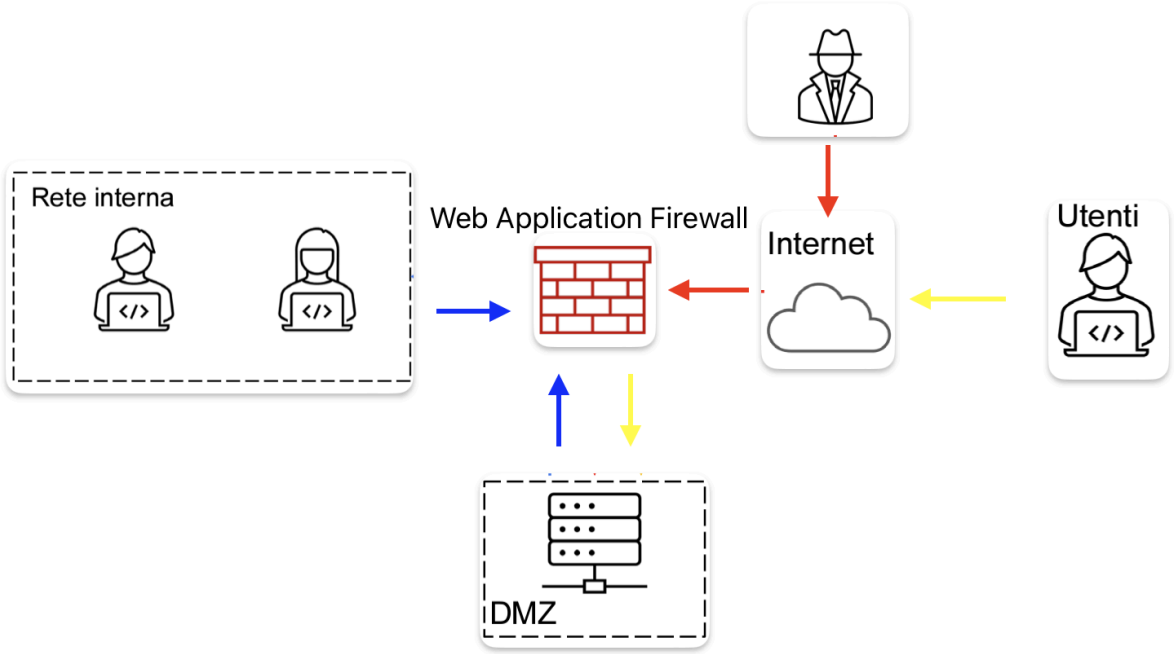
1. Azioni preventive per difendere l'applicazione Web da attacchi SQL e XSS

Le azioni preventive da implementare sono le seguenti:

-Implementazione di controlli di accesso; I controlli di accesso garantiscono che solo gli utenti autorizzati possano accedere alla propria rete, applicazioni Web.

-Implementazione di un firewall; Il firewall consente di filtrare il traffico in entrata e in uscita dalla rete, bloccando le connessioni non autorizzate.

-Installazione di un antivirus; L'antivirus protegge la rete da malware, che possono essere utilizzati per lanciare attacchi SQL e XSS.
-Installazione di un sistema IPS/IDS; L'IPS/IDS monitora il traffico di rete per rilevare attività sospette, che potrebbero indicare un attacco in corso e supporta anche azioni di prevenzione automatiche.
-Validazione e sanitizzazione degli input utente; La validazione e la sanitizzazione degli input utente consentono di rimuovere il codice dannoso dagli input utente prima che venga elaborato dall'applicazione.
-Patching dei sistemi; Sistema e software aggiornati, grazie alle ultime patch di sicurezza che proteggono dalle vulnerabilità note, forniscono maggiore sicurezza..
-Formazione degli utenti sulla sicurezza informatica; Gli utenti formati sulla sicurezza informatica sono più consapevoli delle minacce e sono in grado di identificare e segnalare attività sospette.



2. Impatti sul business di un attacco DDoS

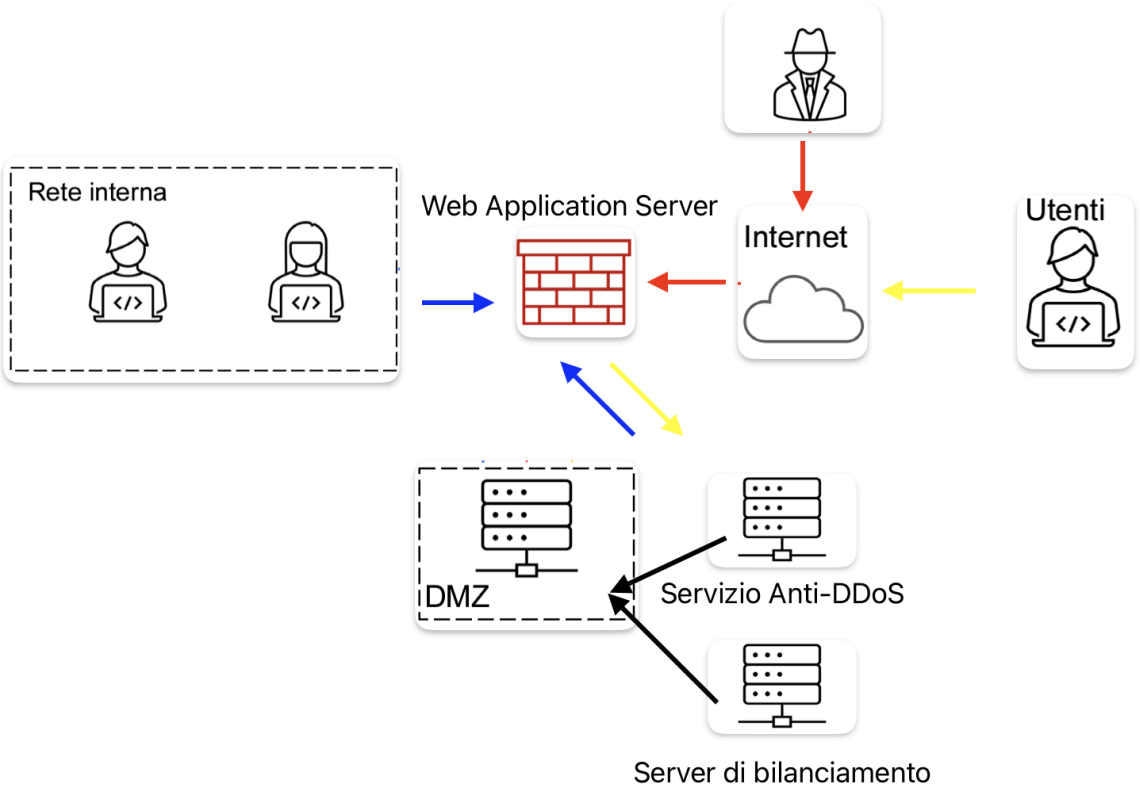
Un attacco DDoS può avere un impatto significativo, causando i seguenti danni:

-Perdita di fatturato; Se l'applicazione Web non è disponibile, gli utenti non possono effettuare acquisti, comportando una perdita di fatturato.
-Danno alla reputazione; Può danneggiare la reputazione dell'azienda, facendola sembrare inaffidabile.
-Costi per la ripresa; La ripresa da un attacco DDoS può essere costosa, in quanto richiede l'intervento di esperti di sicurezza informatica. Se l'applicazione Web

non è raggiungibile per **10 minuti** e gli utenti spendono in media **1.500 €** sulla piattaforma di e-commerce ogni minuto, l'impatto è di **15.000 €.**

Per ridurre l'impatto è possibile implementare le seguenti misure preventive:

Utilizzo di un servizio Anti-DDoS: Un servizio di mitigazione DDoS può reindirizzare il traffico dannoso lontano dall'applicazione Web.
Implementazione di un bilanciamento del carico: Il bilanciamento del carico distribuisce il traffico su più server, il che rende più difficile per un attacco DDoS sopraffare un singolo server.
Sviluppo di un piano di Disaster Recovery: Un piano di ripresa da un disastro fornisce le istruzioni su come ripristinare l'applicazione Web dopo un attacco DDoS.



3. <u>Response a un'infezione da malware</u>

La priorità è impedire la propagazione del malware sulla rete. Le azioni che possono essere intraprese sono:

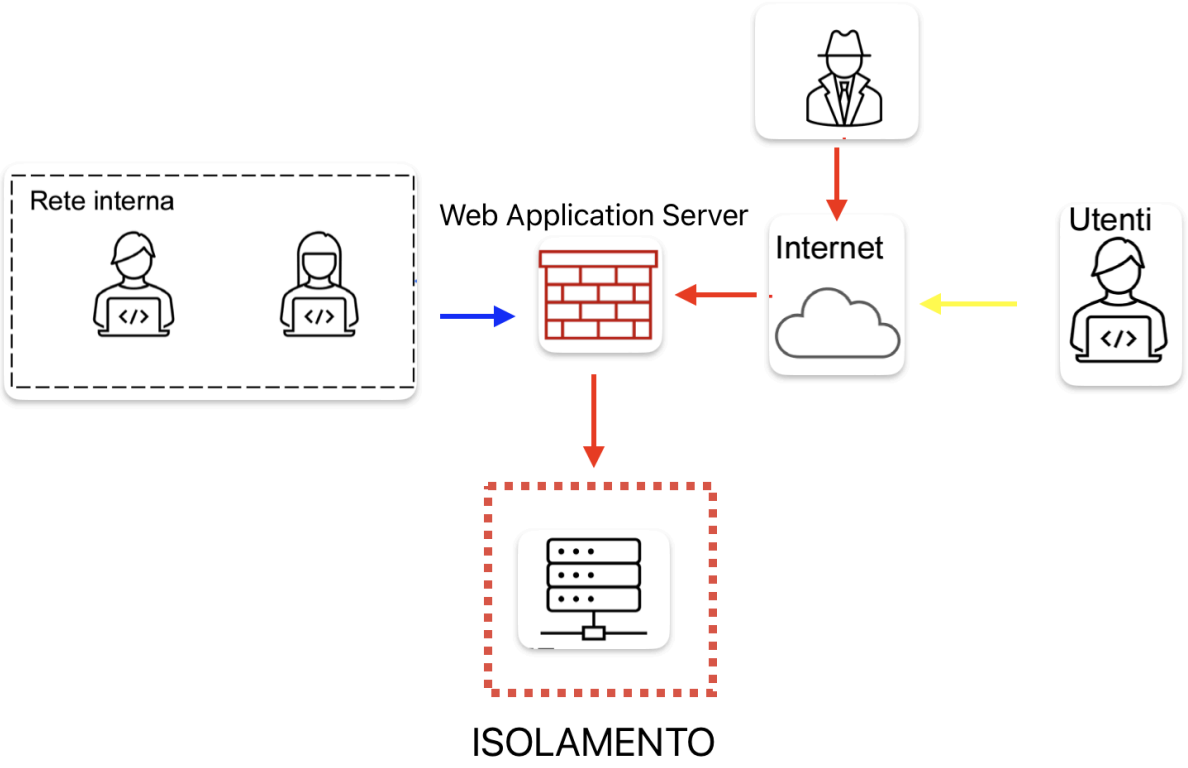
-Isolare la macchina infetta; La macchina infetta deve essere isolata dalla rete per impedire la propagazione del malware ad altri sistemi.

-Disattivare l'accesso remoto; L'accesso remoto alla macchina infetta deve essere disattivato così da impedire all'attaccante di utilizzarlo per diffondere il malware.

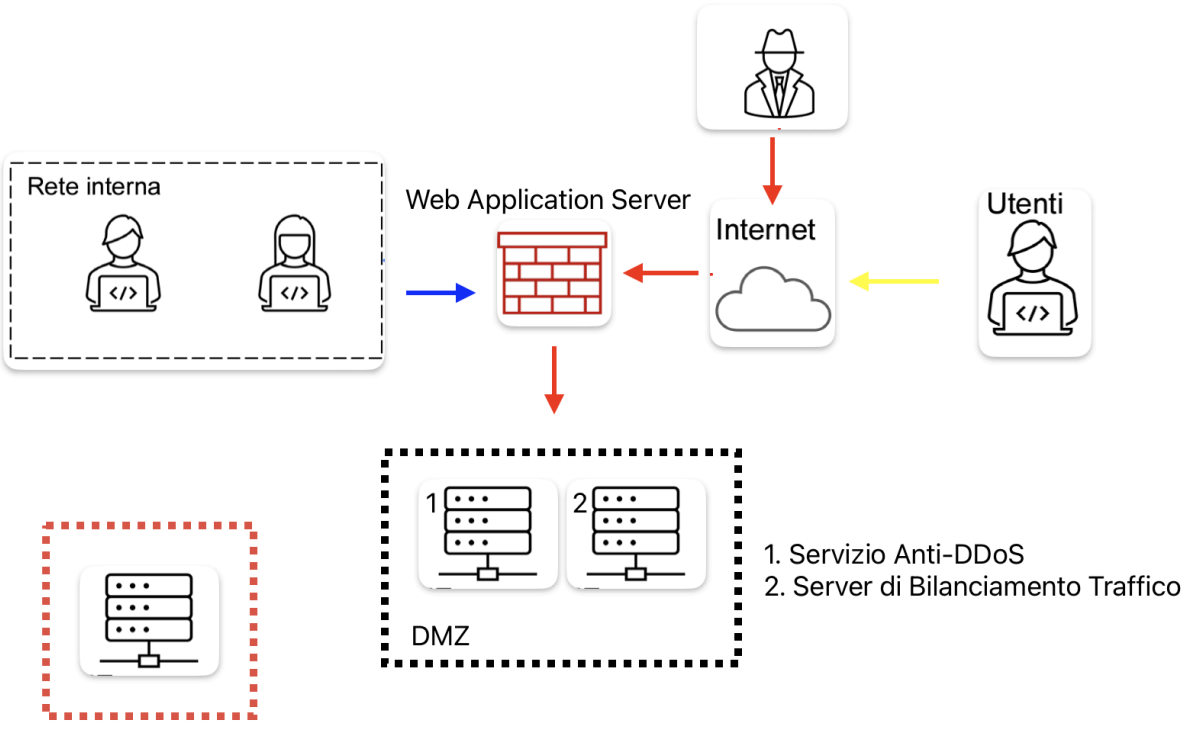
-Analizzare la macchina infetta; Deve essere fatta un' analisi per identificare il malware e comprenderne il modo di propagazione.

-Rimuovere il malware; Il malware deve essere rimosso dalla macchina infetta.

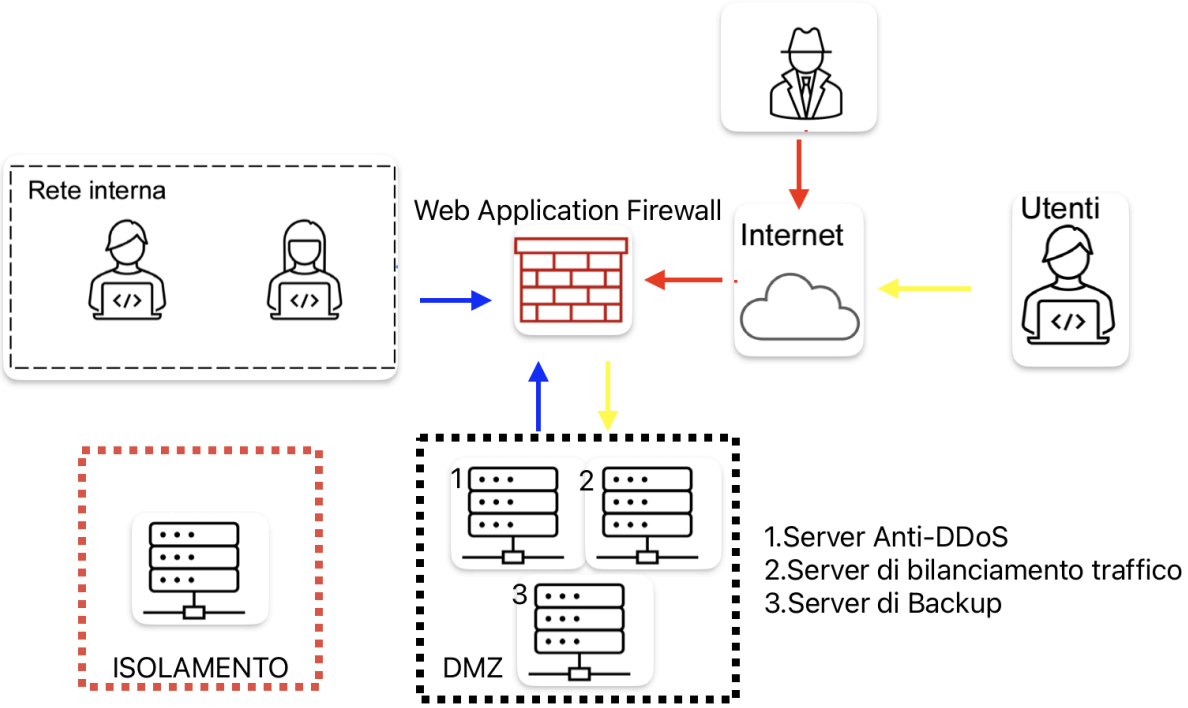
-Ripristinare i sistemi compromessi; I sistemi compromessi dal malware devono essere ripristinati da backup sicuri.



4.



5. E’ stato inserito ulteriormente un server di backup così da garantire la disponibilità dei dati.

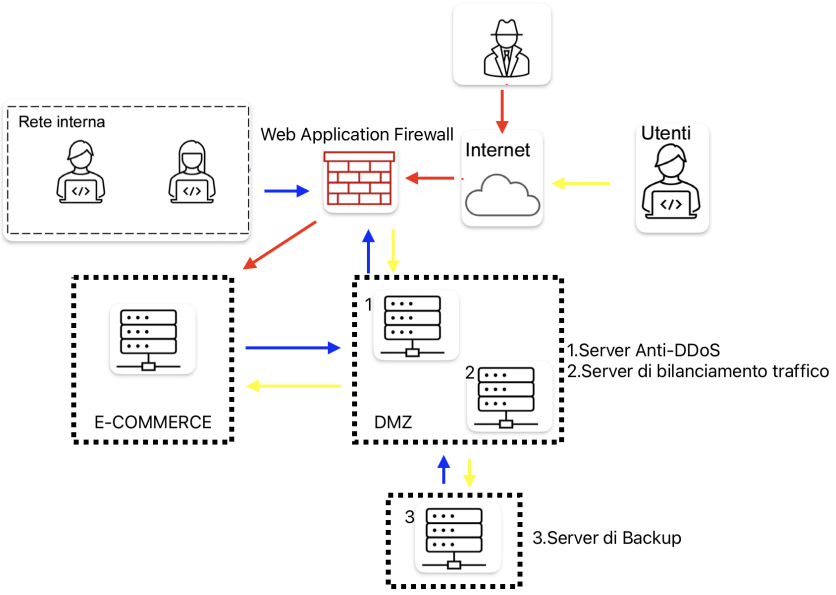


Altre implementazioni:

Crittografia dei dati: Diminuisce la possibilità di violazione dei dati.

Controllo degli accessi basato sui ruoli: Concede agli utenti solo i permessi necessari per svolgere le proprie mansioni.

Segmentazione della rete: Divide la rete in segmenti separati per limitare la propagazione di malware.



BONUS:

La *prima* analisi ci porta a pensare che il malware raccolga informazioni di sistema e ne crea una copia facendola passare per un backup. Inoltre esso modifica le policy della powershell, i permessi di alcuni file e directory e scannerizza i software presenti sul sistema

La *seconda* analisi sembrerebbe un normale aggiornamento se non fosse per la sorgente di provenienza. Esso legge le specifiche del browser, disabilita il SEHOP(Structured Exception Handler Overwrite Protection),che consiste in una tecnica utilizzata per prevenire la possibilità di attacchi che sfruttano la tecnica dello Structured Exception Handler (SEH) Overwrite, ovvero la sovrascrittura di un blocco di codice preposto alla gestione delle eccezioni che possono verificarsi durante la normale elaborazione di un'applicazione ed infine droppa gli eseguibili legittimi di windows.

Per non incappare in questo genere di situazioni bisogna sempre controllare la provenienza dei file scaricati. Quando non si può arrivare ad essere sicuri,l'implementazione di un antivirus che controlli il file in cerca di possibili malware, è una delle soluzioni. L’aggiunta del firewall può certamente aiutare ad evitare accessi indesiderati ed a contrastare possibili situazioni critiche.