11.07.2025

SECURITY OPERATION

PROGETTO FINE MODULO M5

FABIO MUNGIOVÌ

SECURITY OPERATION

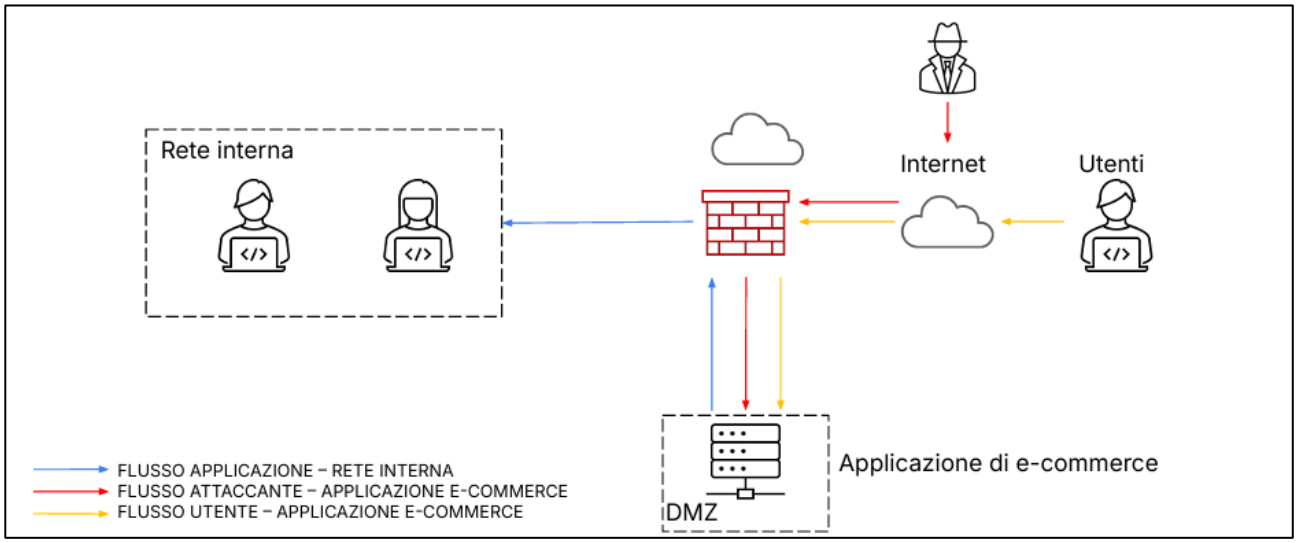
PROGETTO FINE MODULO M5

INDICE

INTRODUZIONE

Il presente report ha lo scopo di analizzare l'architettura di rete di un'applicazione di e-commerce e di proporre una serie di interventi mirati a migliorarne la sicurezza, agendo sia sul piano preventivo che su quello della risposta agli incidenti.

L'analisi si riferisce da uno scenario aziendale che vede un'applicazione web, ospitata in una Zona Demilitarizzata (DMZ), esposta a minacce provenienti da Internet e con una configurazione di rete che permette una potenziale comunicazione verso la rete interna aziendale.



Il report si sviluppa attraverso la risoluzione di alcuni quesiti, con lo scopo di analizzare diverse metodologie di implementazione di sistemi di sicurezza informatica applicati a questo contesto.

Nel dettaglio, verranno affrontati i seguenti punti:

- **Azioni Preventive**: Si analizzeranno le strategie e gli strumenti più efficaci per difendere l'applicazione da attacchi comuni a livello applicativo, come l'SQL Injection (SQLi) e il Cross-Site Scripting (XSS).
- **Impatto sul Business**: Verrà quantificato il danno economico derivante da un attacco di tipo Distributed Denial of Service (DDoS) che causa un'interruzione del servizio per 10 minuti, considerando una perdita media di 1.500 € al minuto.
  Verranno inoltre valutate le relative contromisure.
- **Risposta agli Incidenti (Response):** Sarà delineata una strategia di contenimento per un'infezione malware sul server web, con la priorità assoluta di impedire la propagazione alla rete interna.
- **Soluzioni Architetturali**: Infine, verranno presentate due proposte di revisione dell'infrastruttura: una prima soluzione che unisce le misure preventive e di contenimento e una seconda, "più aggressiva", che delinea un'architettura di sicurezza avanzata.

Ogni sezione fornirà una soluzione mantenendo l'ottica di una media impresa che deve bilanciare investimenti e livello di protezione.

1. AZIONI PREVENTIVE CONTRO ATTACCHI SQLi e XSS

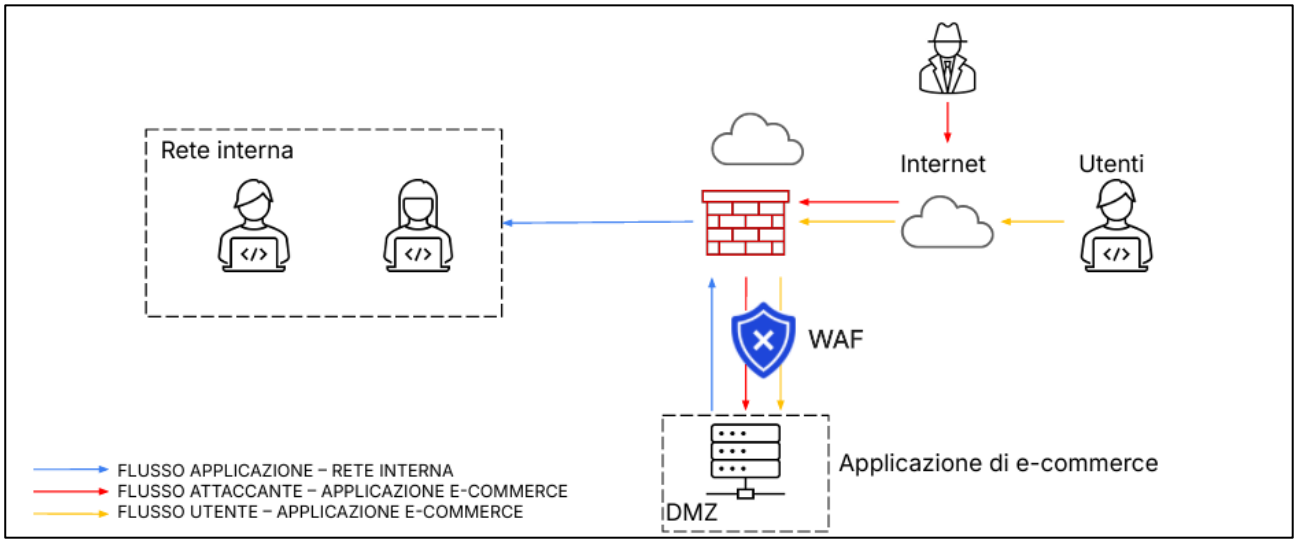
Per proteggere l'applicazione web da attacchi comuni come **SQL Injection (SQLi)** e **Cross-Site Scripting (XSS),** non è sufficiente affidarsi unicamente al firewall perimetrale, che opera principalmente a livello di rete (layer 3 e 4 del modello OSI) e non è specializzato nell'analisi del traffico applicativo (layer 7).

La soluzione più efficace consiste nell'introdurre un **Web Application Firewall (WAF)**.
Questo dispositivo o servizio software è specificamente progettato per ispezionare il traffico HTTP/HTTPS diretto verso l'applicazione web.
Funziona come un filtro avanzato che, basandosi su un set di regole e firme è in grado di identificare e bloccare richieste malevole che contengono payload di attacchi SQLi, XSS e altre vulnerabilità note a livello applicativo.

Implementazione nell'architettura

Il **WAF** andrebbe posizionato all'interno della DMZ, tra il firewall perimetrale e il server dell'applicazione di e-commerce.
In questo modo, tutto il traffico degli utenti (e degli attaccanti), dopo aver superato il primo filtro del firewall di rete, verrebbe ispezionato in modo approfondito dal **WAF** prima di raggiungere l'applicazione.

Questo aggiunge un livello di difesa che protegge direttamente il codice dell'applicazione.



Secure Coding

Oltre al WAF, è fondamentale che gli sviluppatori adottino pratiche di **codifica sicura (secure coding).**

Tecniche come l'utilizzo della validazione e sanificazione di tutti i dati forniti dall'utente sono misure indispensabili che rendono l'applicazione più robusta.

Il WAF agisce come uno scudo, ma la sicurezza migliore nasce direttamente dal software.

2. IMPATTO SUL BUSINESS DI UN ATTACCO DDoS

Un attacco di tipo **Distributed Denial of Service (DDoS)** ha lo scopo di esaurire le risorse di un servizio fino a renderlo inaccessibile.

In questo scenario, l'impatto economico è diretto e facilmente calcolabile.

- **Durata dell'interruzione del servizio**: 10 minuti.
- **Perdita media al minuto**: 1.500 €.

Il calcolo dell'impatto totale sul business è quindi:

Impatto Totale = 10 minuti×1.500 €/minuto = 15.000 €

Un'interruzione di soli dieci minuti causerebbe una perdita diretta di **15.000 €.**

A questa cifra andrebbero aggiunti i costi indiretti, spesso più difficili da quantificare, come il danno alla reputazione del brand, la perdita di fiducia da parte dei clienti e il possibile abbandono della piattaforma a favore di concorrenti.

Azioni preventive:

Affrontare un attacco DDoS con le sole risorse interne è quasi impossibile per una media impresa, data l'enorme volume di traffico che questi attacchi possono generare.

La strategia migliore è affidarsi a un servizio di mitigazione DDoS basato su cloud.
Questi servizi funzionano deviando tutto il traffico destinato all'azienda attraverso la loro rete globale che ha la capacità di assorbire e "pulire" il traffico, filtrando quello malevolo e lasciando passare solo le richieste legittime degli utenti.

Questa soluzione viene implementata "a monte" del firewall aziendale, proteggendo l'intera connessione a Internet.

3. RISPOSTA A UN INFEZIONE MALWARE E CONTENIMENTO

Lo scenario descrive un'infezione da malware sul server di e-commerce nella DMZ, con la priorità assoluta di impedire che l'infezione si propaghi alla rete interna.

La parte critica dell'architettura attuale è che la rete interna è raggiungibile dalla DMZ.

Questa è una configurazione estremamente pericolosa che annulla in parte lo scopo della DMZ.

La DMZ dovrebbe essere una “zona cuscinetto” isolata, i sistemi al suo interno non dovrebbero mai avere la possibilità di iniziare connessioni verso la rete interna.

Soluzione di contenimento:

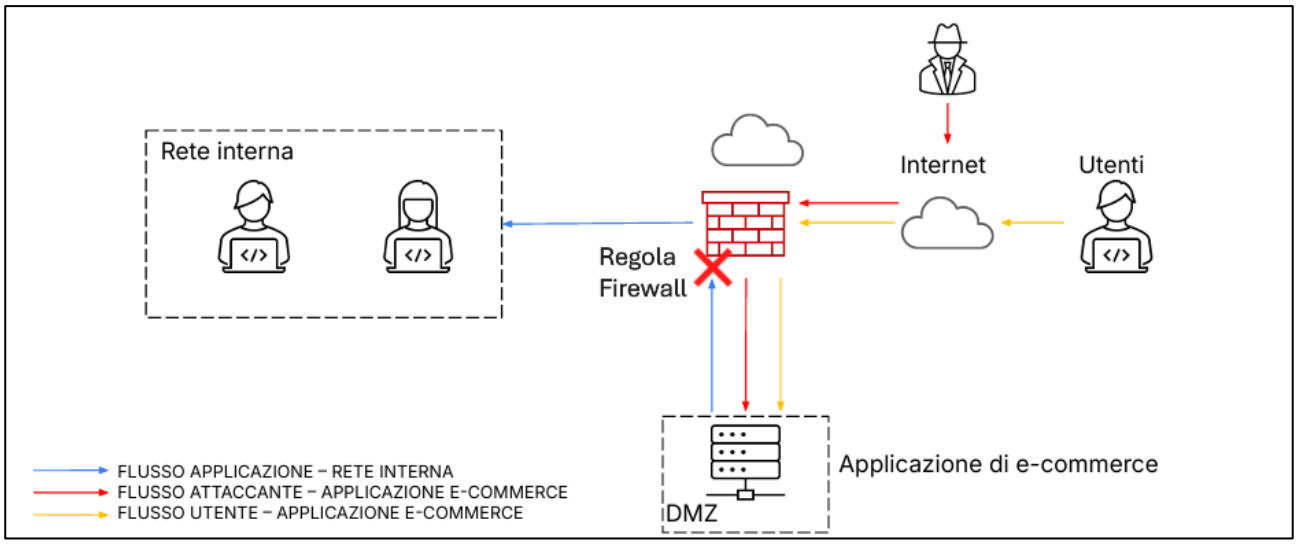
La risposta immediata e fondamentale è una modifica delle regole del firewall.

Si deve implementare una regola che nega categoricamente qualsiasi connessione iniziata dalla DMZ verso la rete interna.
Sono permesse solo le connessioni che seguono la direzione opposta: dalla rete interna verso la DMZ (ad esempio, per permettere agli amministratori di sistema di gestire il server) e, ovviamente, da Internet verso la DMZ.

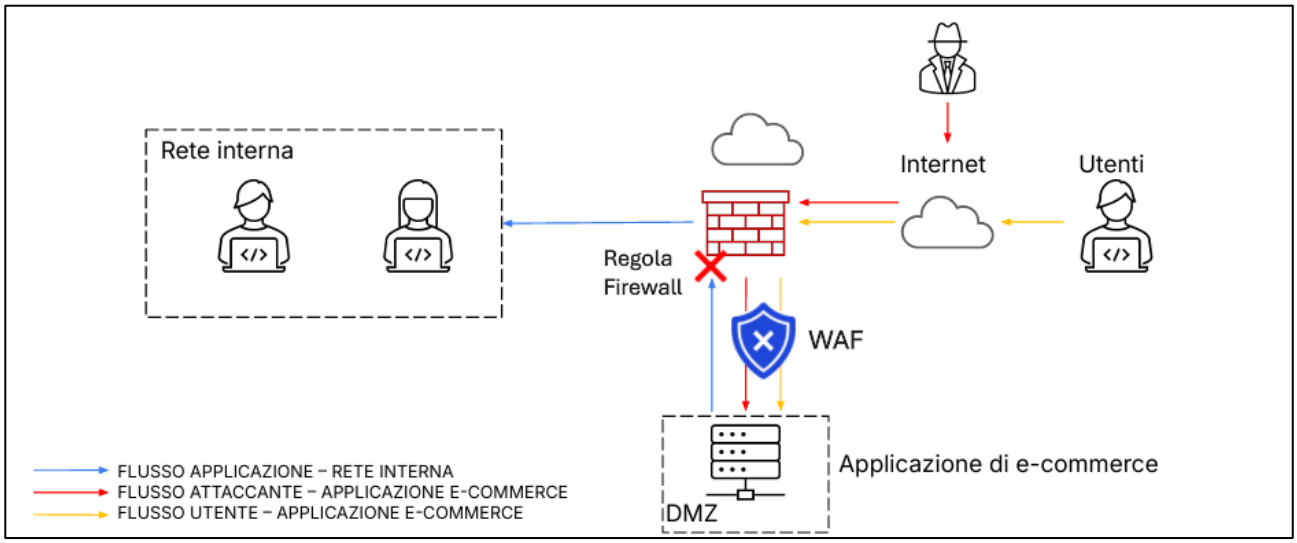
Implementazione nell'architettura:

Nella figura, il flusso rappresentato dalla freccia blu ("FLUSSO APPLICAZIONE - RETE INTERNA") che va dalla DMZ alla rete interna deve essere bloccato a livello del firewall.

Questa modifica di configurazione è l'azione più critica per il contenimento, perché anche se l'attaccante ha il pieno controllo del server in DMZ, non avrà un percorso di rete per raggiungere e infettare le macchine della rete interna.



4. SOLUZIONE COMPLETA (Unione delle Soluzioni 1 e 3)



La figura illustra l'architettura di rete modificata per implementare la soluzione completa, che unisce le misure preventive del quesito 1 con le azioni di risposta e contenimento del quesito 3.

Le modifiche rappresentate sono due:

1. **Introduzione di un Web Application Firewall (WAF)**: All'interno della DMZ, è stato inserito un WAF tra il firewall perimetrale e il server di e-commerce.
   Questo componente ispeziona tutto il traffico web per proteggere l'applicazione da attacchi specifici come SQL Injection e Cross-Site Scripting (XSS).
   Il suo posizionamento garantisce che le richieste malevole vengano filtrate prima di raggiungere il server.
2. **Rinforzo della Segmentazione di Rete**: È stato applicato un blocco al flusso di comunicazione che dalla DMZ si dirigeva verso la Rete Interna.
   Questa modifica della regola del firewall, visualizzata nell'immagine, è fondamentale per il contenimento degli incidenti.
   In caso di compromissione del server web a causa di un malware, questa separazione impedisce all'attaccante di propagare l'infezione e muoversi lateralmente verso le risorse critiche della rete aziendale.

Questa configurazione crea una difesa a più livelli, dove la sicurezza dell'applicazione e l'isolamento della rete lavorano insieme per fornire una protezione robusta ed efficace.

5. PROPOSTA DI MODIFICA “PIU’ AGGRESSIVA” DELL’INFRASTRUTTURA

Una modifica "più aggressiva" va oltre la semplice correzione dei problemi esistenti e mira a costruire un'infrastruttura più sicura e resiliente.

Questa visione è adatta a un'impresa che considera la sicurezza informatica un investimento strategico.

Ecco gli elementi di una tale architettura avanzata:

- **Servizio di Mitigazione DDoS in Cloud:**
  Come prima linea di difesa, tutto il traffico Internet verrebbe instradato attraverso un provider specializzato in protezione DDoS. Questo scudo esterno assorbirebbe gli attacchi volumetrici prima che possano raggiungere l'infrastruttura aziendale, garantendo la continuità del servizio di e-commerce.

- **Introduzione di un Bastion Host (o Jump Server):**
  Per eliminare completamente i rischi legati all'accesso amministrativo, si potrebbe implementare un **bastion host**.
  Si tratta di un server "sacrificale", estremamente fortificato e monitorato, posizionato nella DMZ.
  Qualsiasi amministratore della rete interna che necessiti di gestire il server di e-commerce non si connetterebbe più direttamente, ma dovrebbe prima accedere in modo sicuro a questo bastion host, e solo da lì "saltare" sul server da amministrare.
  Questo crea un unico punto di accesso controllato e tracciato, riducendo molto la superficie d'attacco.

- **Implementazione di un Sistema IDS/IPS:**
  Si potrebbe aggiungere un **Intrusion Detection/Prevention System (IDS/IPS).**
  Questo sistema non si limita a filtrare il traffico in base a regole fisse come un firewall, ma lo analizza in tempo reale alla ricerca di comportamenti anomali o firme di attacchi noti. Potrebbe essere posizionato a "ridosso" del firewall per monitorare tutto il traffico da e per la DMZ, fornendo una capacità di rilevamento e, nel caso di un IPS, di blocco attivo delle minacce.

Questa architettura "aggressiva" trasforma la sicurezza da un approccio puramente reattivo a uno proattivo, basato sui principi di **difesa in profondità (defense in depth) e Zero Trust**, dove ogni accesso viene verificato e il traffico costantemente monitorato alla ricerca di anomalie.