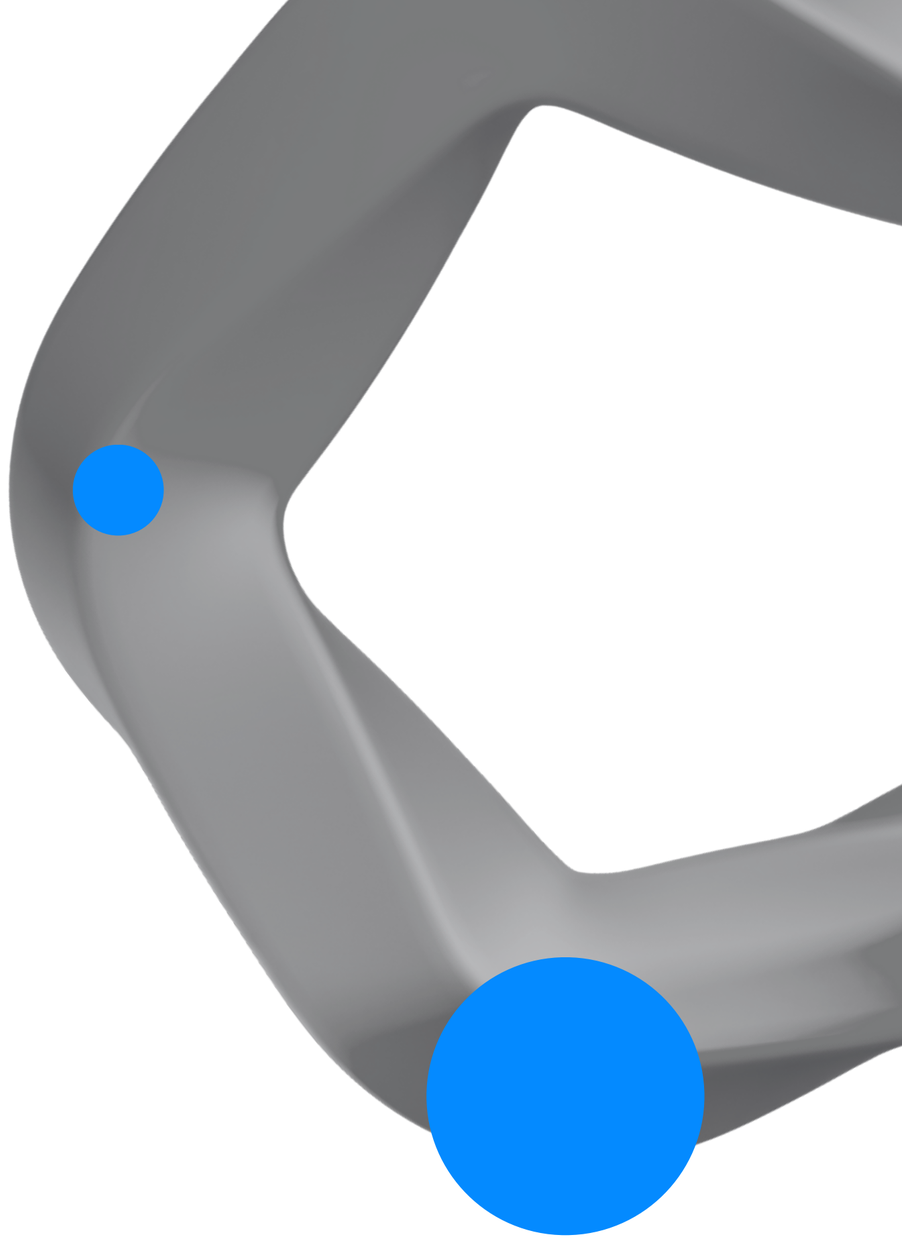
Gabriele
Genovesi



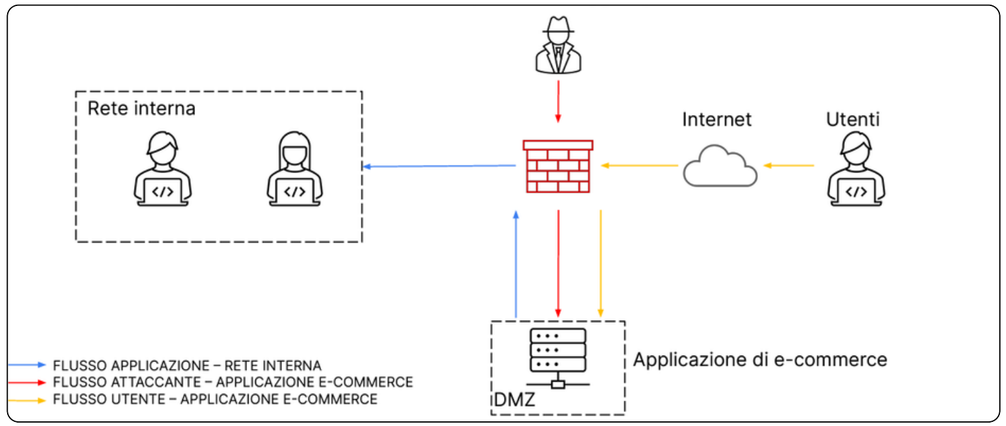
Progetto week_9

Simulazione attacco

Introduzione:

CON RIFERIMENTO ALLA FIGURA 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.
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.



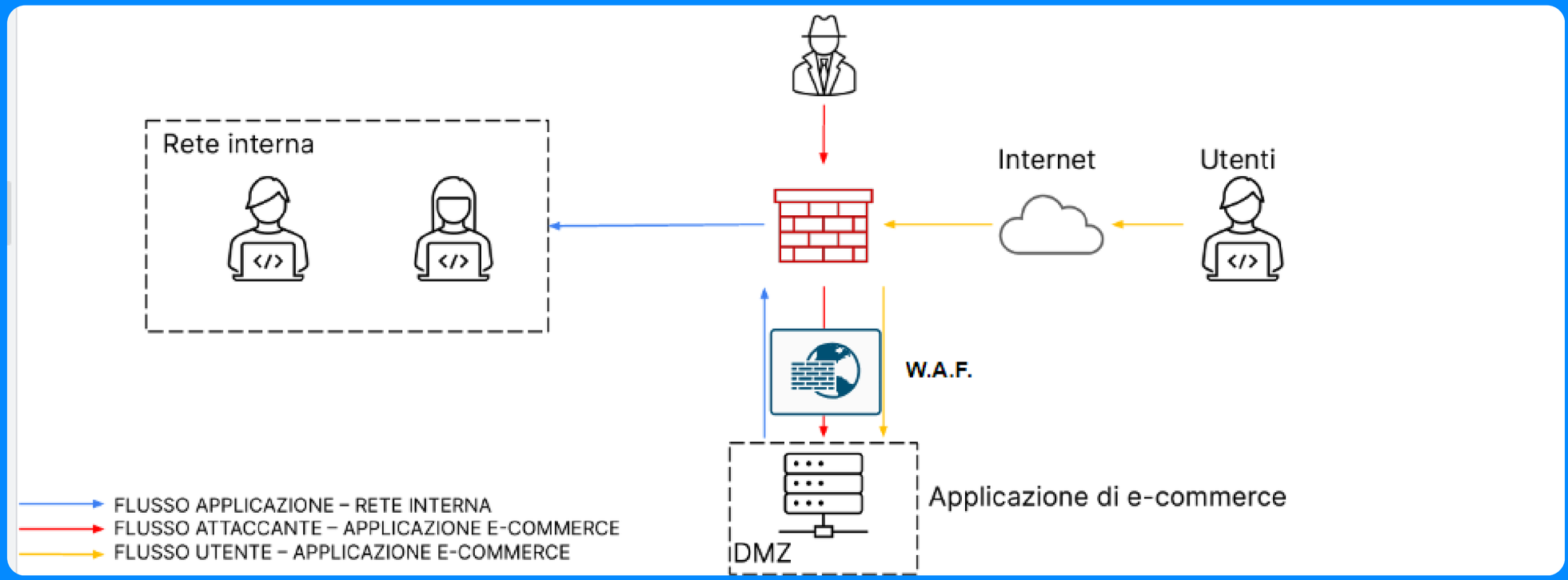
1. Azioni preventive

Cosa si intende per azioni preventive? Si includono nelle azioni preventive tutte quelle azioni di sicurezza che vengono adottate ed implementate anticipatamente e preventivamente per ridurre i rischi di eventi negativi, (Sostanzialmente l'opposto delle azioni correttive, azioni di rimedio a stretto giro per risolvere gli incidenti e ripristinare il corretto funzionamento dei sistemi informativi quanto prima possibile).

SQLi?
SQL Injection (SQLi) è un attacco informatico che sfrutta campi di input per eseguire comandi SQL dannosi, compromettendo la sicurezza e consentendo l'accesso non autorizzato ai database. La prevenzione coinvolge l'uso di pratiche di sviluppo sicure e la consapevolezza degli sviluppatori.

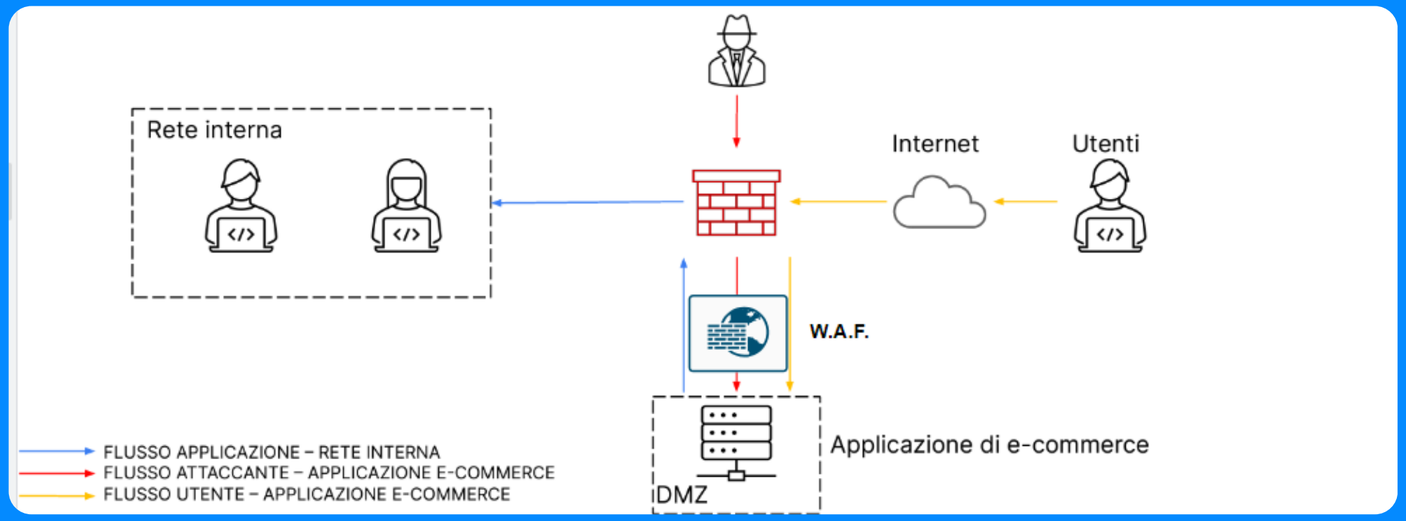
XSS? Un attacco XSS (Cross-Site Scripting) coinvolge l'inserimento di script dannosi da parte di un attaccante all'interno di pagine web visualizzate da altri utenti. Ciò consente all'attaccante di eseguire codice lato client sul browser delle vittime, compromettendo la sicurezza dell'applicazione e facilitando il furto di informazioni sensibili. La prevenzione di XSS richiede validazione e encoding accurati dei dati di input.

1 Parte pratica



Implementare un **Web Application Firewall (WAF)** è un'opzione corretta e spesso consigliata come parte di una strategia di sicurezza per proteggere un'applicazione web (Come aggiunto in figura). Un WAF è uno strumento progettato per filtrare, monitorare e bloccare il traffico HTTP/HTTPS tra un'applicazione web e il web.

1 Parte pratica

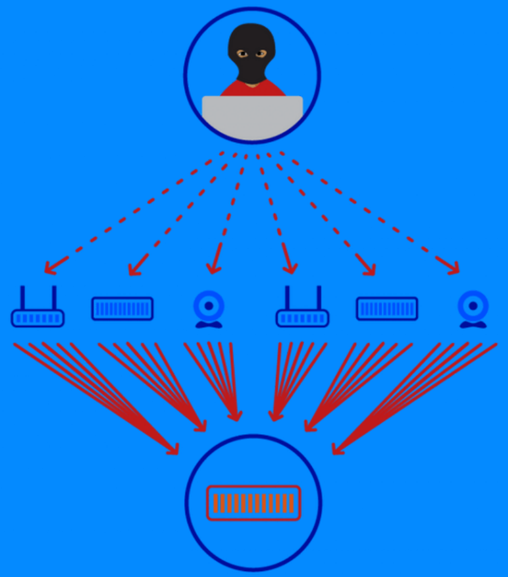


Non è l'unica procedura attuabile per difendere l'**applicazione Web** da attacchi di tipo **SQLi** oppure **XSS** vengono consigliate, specialmente a livello web le seguenti pratiche:
- Verificare e validare i dati di input degli utenti. - Utilizzare i parametri nelle query SQL per evitare l'iniezione di codice
-Verificare che i dati inseriti dagli utenti siano conformi a specifici criteri. In questo modo, gli utenti non saranno in grado di inserire codice malevolo come parte dei dati di input.
- Utilizzare librerie di sicurezza specifiche per la gestione delle vulnerabilità XSS e SQLi.
-Configurare correttamente il server web per limitare l'accesso ai file e alle cartelle sensibili.
-Formare il personale sulla sicurezza delle applicazioni web e sui rischi associati alle vulnerabilità XSS e SQLi, per ridurre al minimo le possibilità di errore umano.
-Monitorare costantemente l'applicazione web per individuare eventuali attacchi

2. Impatto sul business

Impatti sul business, spesso per valutare e gestire l'impato sul business viene applicato il **Business Countinuity Plan:**
Il Business Continuity Plan (BCP) è un documento strategico che identifica e pianifica le procedure per mantenere la continuità operativa durante eventi come disastri, guasti tecnologici o altri imprevisti. Include analisi del rischio, piani operativi di emergenza e strategie per garantire il ripristino rapido delle attività aziendali.

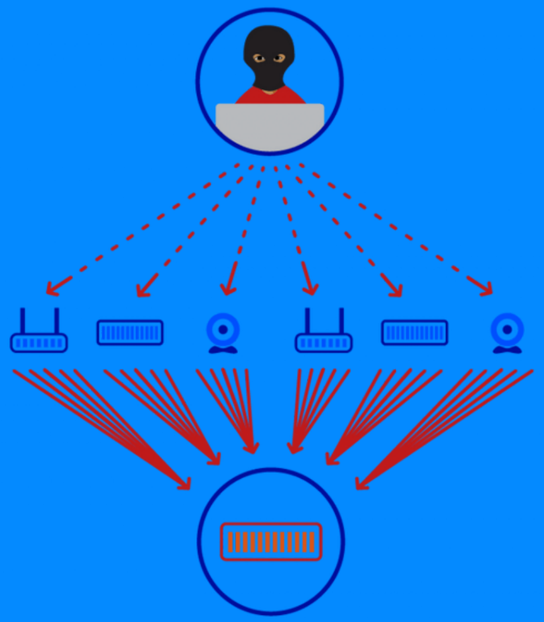
Attacco Ddos? Un attacco DDoS (Distributed Denial of Service) è un tentativo di rendere un servizio, un sito web o una rete inaccessibili sovraccaricandoli con un volume massiccio di richieste, spesso provenienti da una rete distribuita di computer compromessi, con l'obiettivo di sopraffare le risorse e causare un'interruzione del servizio. L'obiettivo principale è negare l'accesso legittimo agli utenti, causando un'indisponibilità del servizio.



2 Parte pratica

L”applicazione Web subisce un attacco di tipo DDoS che rende l’applicazione non raggiungibile per 10 minuti.
Calcolando che l’impatto sul business, alla non raggiungibilità del servizio, è di **1.500 euro ogni minuto,** moltiplicando per il tempo in cui il web server non è raggiungibile, ovvero 10 minuti, otteniamo che il **danno subito è di 15.000 euro**.

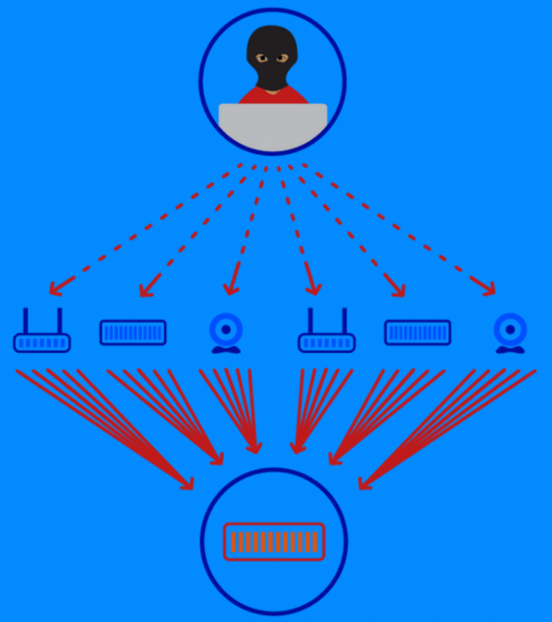
N.B Potremmo associare i 10 minuti al **RTO (Ricovery time objective)** ovvero il tempo impiegato per recuperare una risorsa critica, è bene ricordarci che **RTO** deve essere sempre inferiore o uguale al **MTD,** il tempo massimo che un’azienda può essere non operativa senza subire danni o perdite irreparabili. **RTO <= MTD**



2 Parte pratica

Valutazioni di azioni preventive che si possono adottare.

- Utilizzare un firewall può aiutare a rilevare e mitigare gli attacchi DDoS in tempo reale.
 - Utilizzare un servizio di mitigazione DDoS che sono in grado di rilevare e bloccare gli attacchi DDoS - Ridurre la superficie di attacco delle web app limitando l'accesso solo ai servizi necessari e utilizzando una buona architettura di sicurezza.
- Effettuare test di sicurezza regolari per individuare eventuali vulnerabilità nelle web app. - Pianificare la continuità del servizio in caso di un attacco DDoS, ad esempio utilizzando server di backup o servizi di ridondanza.
- Aggiornare regolarmente i software.
 - Monitorare costantemente il traffico in ingresso e in uscita delle web app.



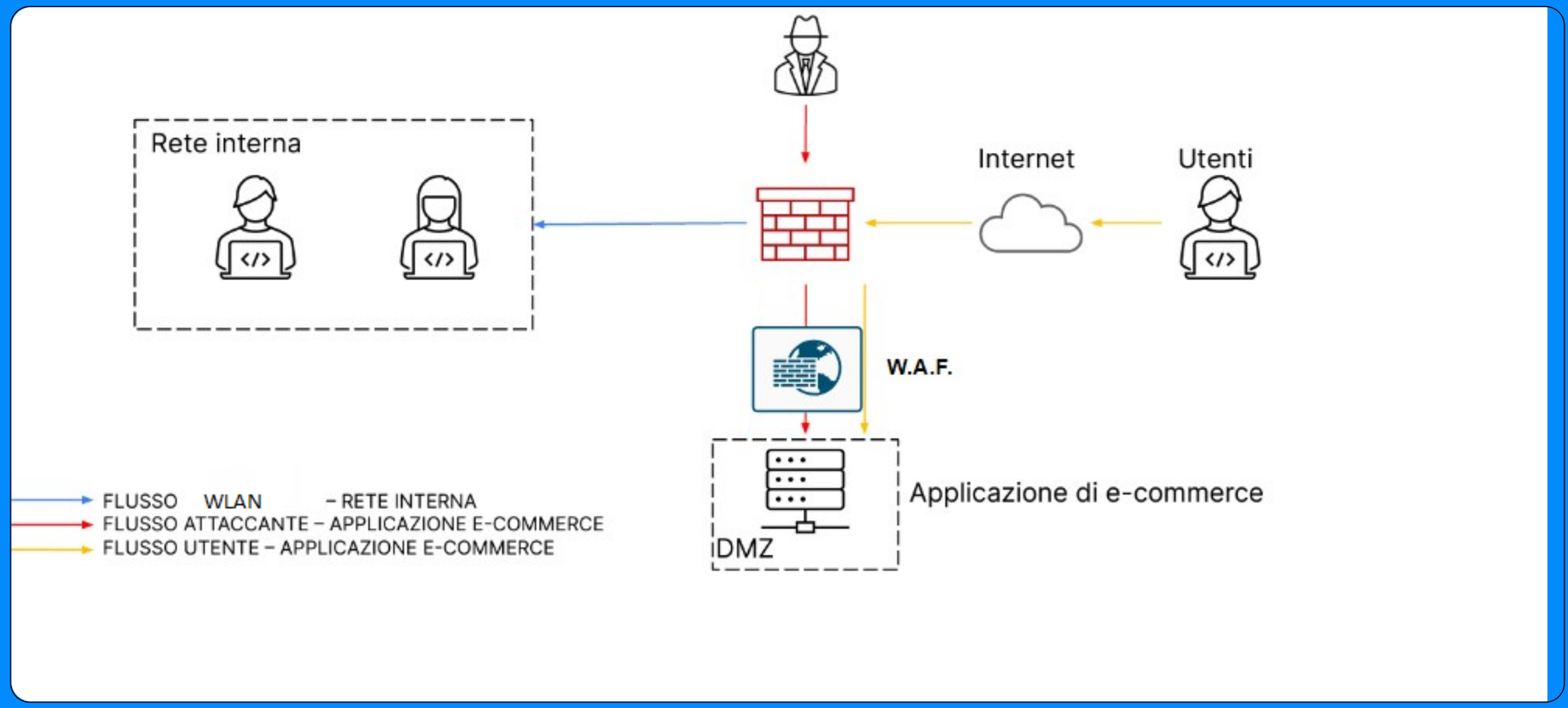
3. Response

Cosa si intende per response: Nel contesto della sicurezza informatica (cybersecurity), il termine "response" si riferisce alle azioni intraprese per affrontare e mitigare una violazione della sicurezza o un incidente informatico. La response è la fase in cui un'organizzazione risponde attivamente a una minaccia per limitare danni, ripristinare l'integrità del sistema e proteggere le risorse digitali.

Ci viene chiesto di supporre la propagazione di un malware all’interno del nostro web server e di avere come priorità la salvaguardia della nostra rete interna quindi di isolare la macchina infetta dalla rete, ma non preoccuparci invece di isolare il web server dall’attaccante (Situazione non molto verosimile e sicuramente non consigliata per la salvaguardia degli utenti)

3 Parte pratica

Isolamento DMZ

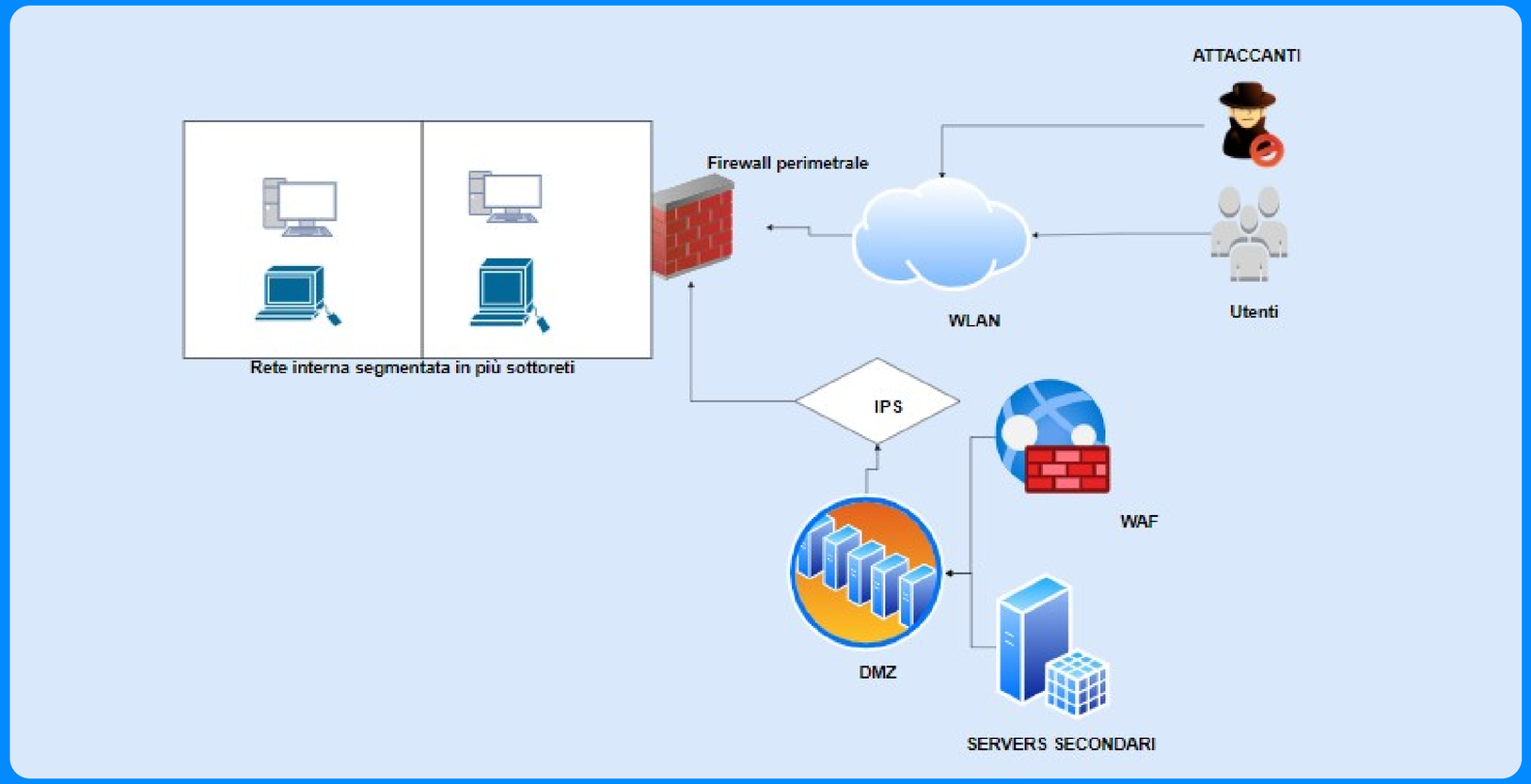


In questo modo riesco ad isolare l’applicazione dalla nostra rete interna per evitarne una diffusione del malware

4. Restrutturazione massiccia della rete

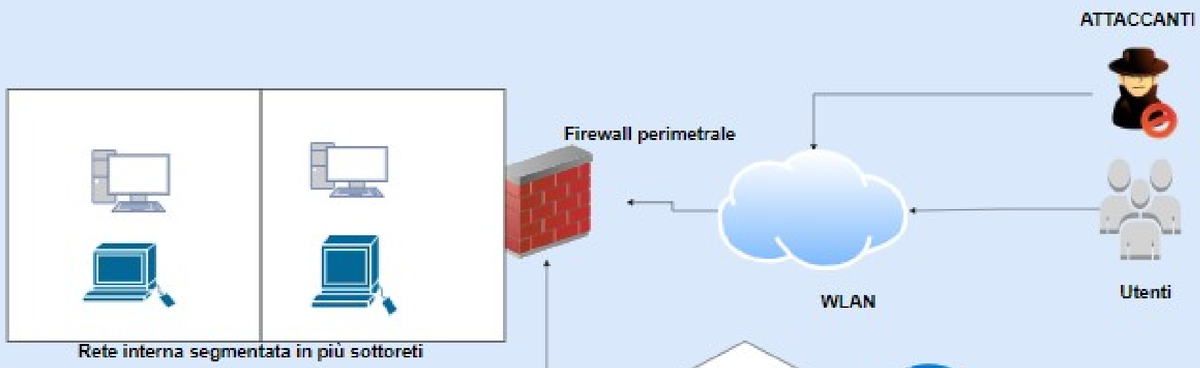
Nuova proposta :

Anche se non richiesto mi sono preso la libertà di ristrutturare lo schema di rete visto nell'esercizio di oggi aggiungendo altri componenti visti durante il nostro corso



4. Restrutturazione massiccia della rete

Nuova proposta :



In questo caso implementiamo configurazioni specifiche del firewall, aggiungiamo un sistema di rilevamento delle intrusioni (IPS) ed un dispositivo di sicurezza per applicazioni Web (WAF). Inoltre possiamo andare a creare una seconda DMZ (Servers secondari) in caso di problemi con la prima DMZ, dovuta ad una compromissione, (Ovviamente la creazione di una seconda DMZ comporta un costo maggiore da sostenere per l'azienda) per garantire ulteriore sicurezza della rete interna nel caso un blackhat riesca ad avervi accesso è stata segmentata in varie sottoreti.

Considerazioni finali

- **Lo schema di rete iniziale** si presenta carente e molto semplificativo dal punto di vista della sicurezza, nel caso un azienda presentasse tale schema consiglierei sicuramente di implementare migliori si stemi di sicurezza.

- **Nel caso venisse infettata la DMZ** il solo isolarla dalla rete interna non rappresenterebbe una soluzione definitia ma anzi lascierebbe tanta libertà agli attaccanti e comporterebbe cattiva pubblicità da parte degli utenti che non verrebbero tutelati in quanto hanno ancora libero accesso alla DMZ Infetta

- **La perdita economic**a non è facilmente quantificabile se elevata o “Trascurabile” perchè non abbiamo altri dati sull’azienda (Se si trattasse di una multinazionale come Google 15'000 euro sarebbero una perdita senza troppo valore)

FINE