EPICODE

CS0424
S9 / L5

ANALISI DEI LOG: CASO REALE

Victoria M. Braile

Prof. Antonio Pozzi

PANORAMICA

Introduzione

01. Analisi preventive contro SQLi e XSS

02. Impatti sul Business

03. Response a infezione da malware

04. Soluzione Completa

05. Modifica più “aggressiva”

06. Conclusioni

INTRODUZIONE

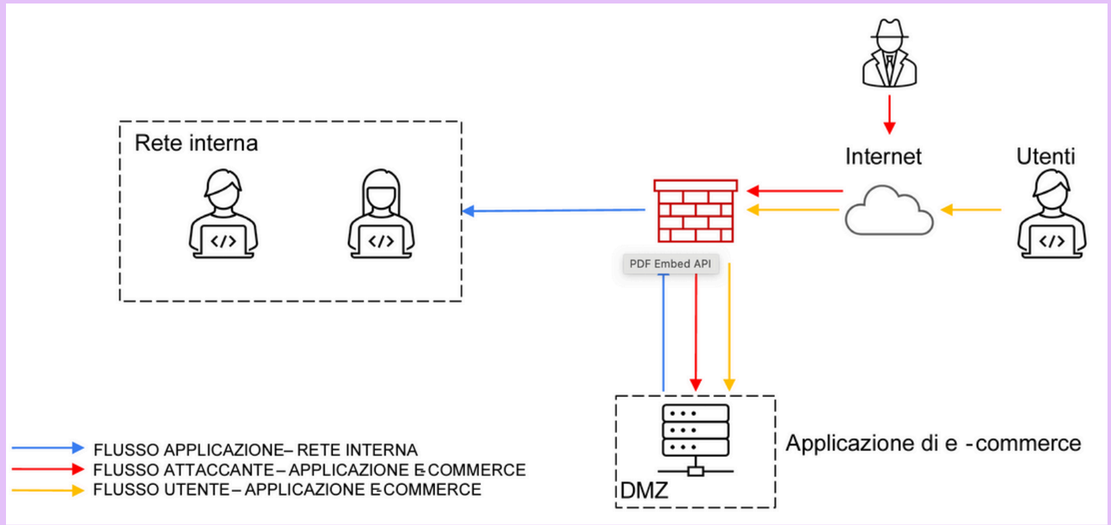
La **sicurezza delle applicazioni web** è una componente cruciale per la protezione dei dati sensibili e per garantire la continuità del servizio agli utenti.
In questo report, viene analizzata un'**architettura di rete** per un'**applicazione di e-commerce** e si risponde a una serie di quesiti relativi alla sicurezza.
L'obiettivo è **identificare e implementare misure preventive** contro attacchi comuni come **SQL Injection (SQLi)** e **Cross-Site Scripting (XSS)**, calcolare l'**impatto di un attacco DDoS** sul **business**, e proporre una soluzione per **isolare un'infezione da malware**. Infine, verrò presentata una **soluzione completa** che integra **tutte le misure preventive e di risposta**, con un'analisi di eventuali modifiche aggiuntive e il relativo **budget**.

ARCHITETTURA DI RETE

L'architettura di rete rappresentata nella figura allegata mostra una configurazione tipica di un'**applicazione di e-commerce**, con una **demilitarized zone (DMZ)** che ospita l'applicazione, **utenti** che accedono dall'esterno, e una **rete interna** per gli **amministratori e sviluppatori**. Identificare e implementare le giuste misure di sicurezza è essenziale per proteggere l'infrastruttura da vari tipi di attacchi.

La figura mostra:

- **Rete interna**: dove risiedono gli **sviluppatori** e **amministratori**.
- **DMZ**: dove è situata l'**applicazione di e-commerce**.
- **Firewall**: che **separa** la **rete interna** e la **DMZ** da Internet.
- **Internet**: da dove provengono sia gli **utenti legittimi** che i **potenziali attaccanti**.
- **Utenti**: che **interagiscono con l'applicazione** di e-commerce.



01.Azioni preventive contro SQLi e XSS

01.1.IMPLEMENTAZIONI CONSIGLIATE

RICHIESTA: quali **azioni preventive** si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo **SQLi** oppure **XSS** da parte di un utente malintenzionato? Modificare la figura per evidenziare le implementazioni.
È richiesta **una sola modifica**.

Le azioni preventive sono **misure implementate per evitare che le vulnerabilità siano sfruttate dagli attaccanti**.
Nel caso specifico, ci si concentra su due tipi di attacchi: **SQLi e XSS**.

Misure Preventive per SQLi

- **Query Parametrizzate**: Utilizzo di query con parametri, prevenendo l'iniezione di comandi malevoli.
- **Validazione degli Input**: Verifica rigorosa degli input ricevuti dagli utenti per assicurarsi che non contengano codice SQL.
- **Web Application Firewall (WAF)**: Firewall che monitora e filtra il **traffico HTTP** per e dalle **applicazioni web**, proteggendo da attacchi comuni come SQLi.

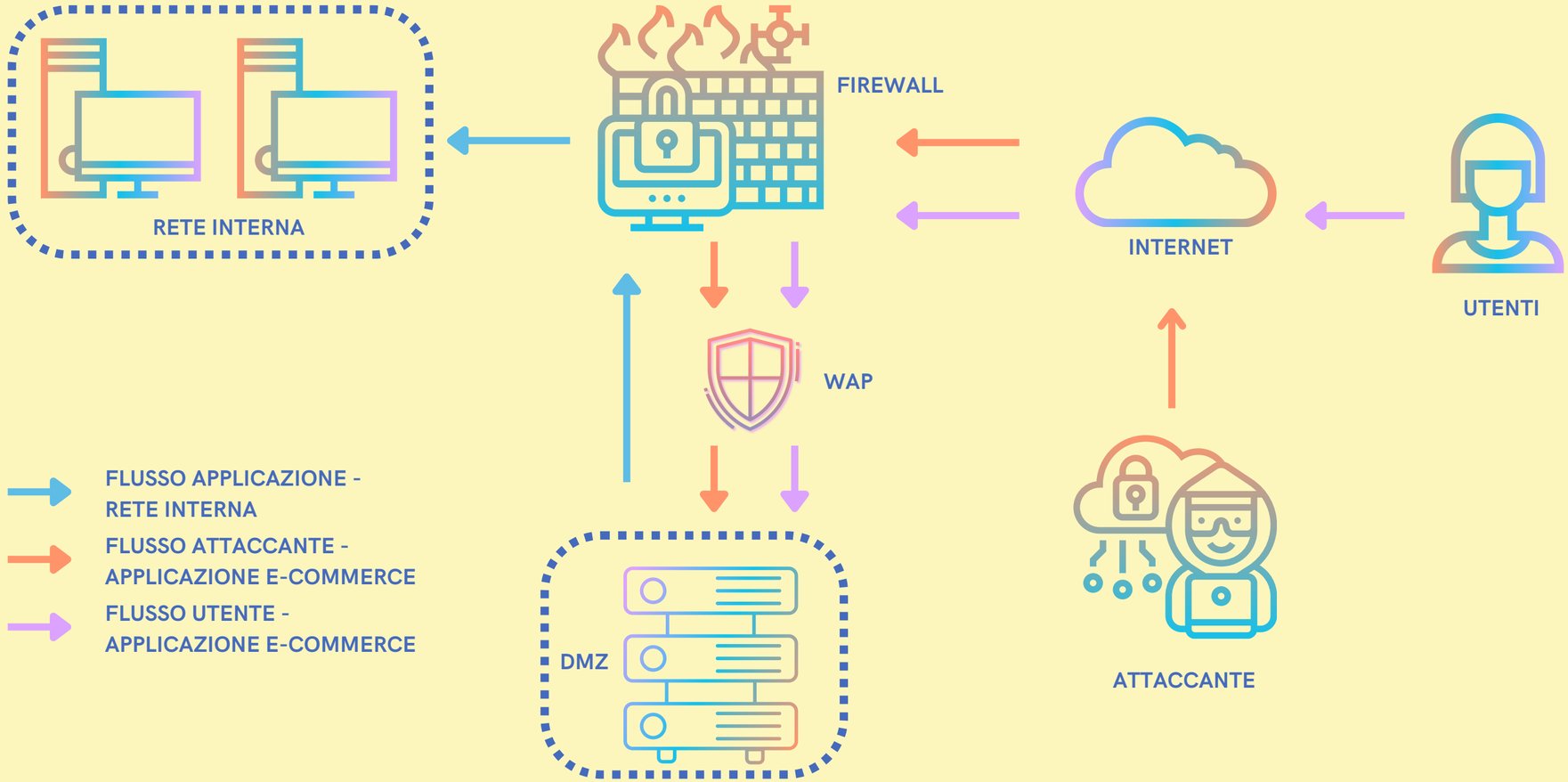
Misure Preventive per XSS

- **Sanitizzazione e Validazione degli Input**: Pulizia e verifica degli input per **rimuovere script malevoli**.
- **HTTPOnly e Secure Flags nei Cookie**: Protezione dei cookie rendendoli inaccessibili agli script lato client.

01.Azioni preventive contro SQLi e XSS

01.2.MODIFICA ARCHITETTURA DI RETE

Per evidenziare queste implementazioni nell'architettura della rete, possiamo aggiungere un **modulo di sicurezza nella DMZ** che rappresenta un **Web Application Firewall (WAF)**. Il WAF è progettato per **filtrare e monitorare il traffico HTTP verso e dall'applicazione web**, fornendo una protezione contro SQLi e XSS.



02.Impatti sul Business

RICHIESTA: l'applicazione Web subisce un **attacco 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 1.200 € sulla piattaforma di e-commerce**.
Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica.

Calcolo dell'impatto DDoS

Se l'applicazione di e-commerce subisce un attacco DDoS che la rende non raggiungibile per 10 minuti, e sapendo che in media gli utenti spendono 1.200 € al minuto, l'impatto sul business è:

Impatto = 10 minuti × 1.200 €/minuto = 12.000 €

Azioni preventive consigliate

- Utilizzare servizi specializzati di **mitigazione DDoS** che distribuiscono il traffico per ridurre l'impatto degli attacchi.
- **Rate Limiting**: limitare il numero di richieste che un utente può fare in un determinato periodo.
- **Load Balancer**: distribuire il traffico su più server per **evitare il sovraccarico di un singolo server**.
- Implementare sistemi di **Monitoraggio e Rilevamento del Traffico Anomalo** per identificare e rispondere rapidamente a comportamenti anomali.

03.Response infezione da malware

03.1.AZIONI DI CONTENIMENTO

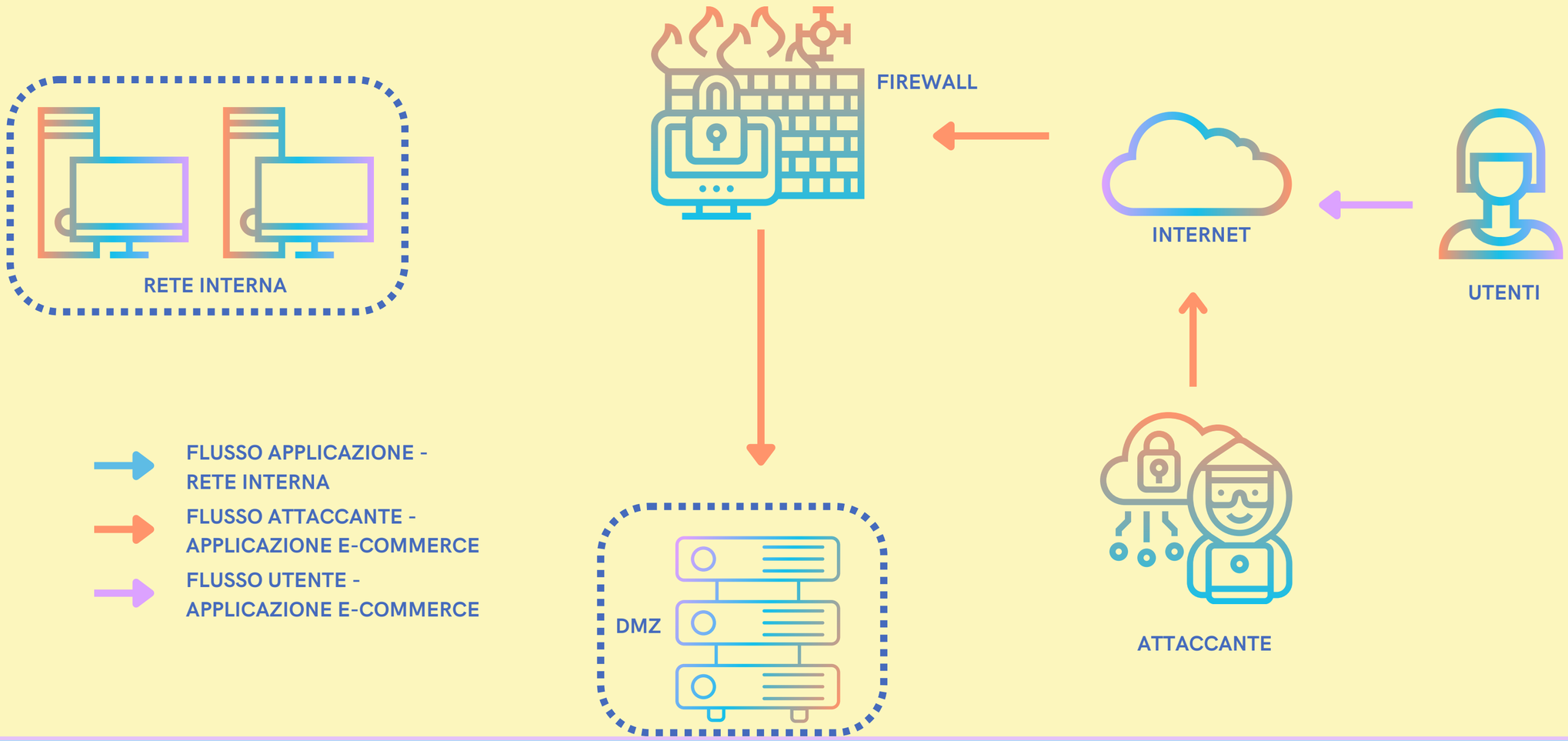
RICHIESTA: l'**applicazione Web** viene **infettata** da un **malware**. La priorità è che il malware **non si propaghi** sulla rete, mentre non serve rimuovere l'accesso da parte dell'attaccante alla macchina infettata.
Modificare l'architettura di rete con la soluzione proposta.

Azioni di Contenimento

- **Isolamento della Macchina Infetta**: Disconnettere la macchina infetta dalla rete per impedire la propagazione del malware.
- **Segmentazione della Rete**: Dividere la rete in segmenti isolati per limitare i movimenti laterali del malware.
- **Configurazione del Firewall**: Aggiornare le regole del firewall per bloccare il traffico sospetto proveniente dalla macchina infetta.

03.Response infezione da malware

03.1.MODIFICA ARCHITETTURA DI RETE

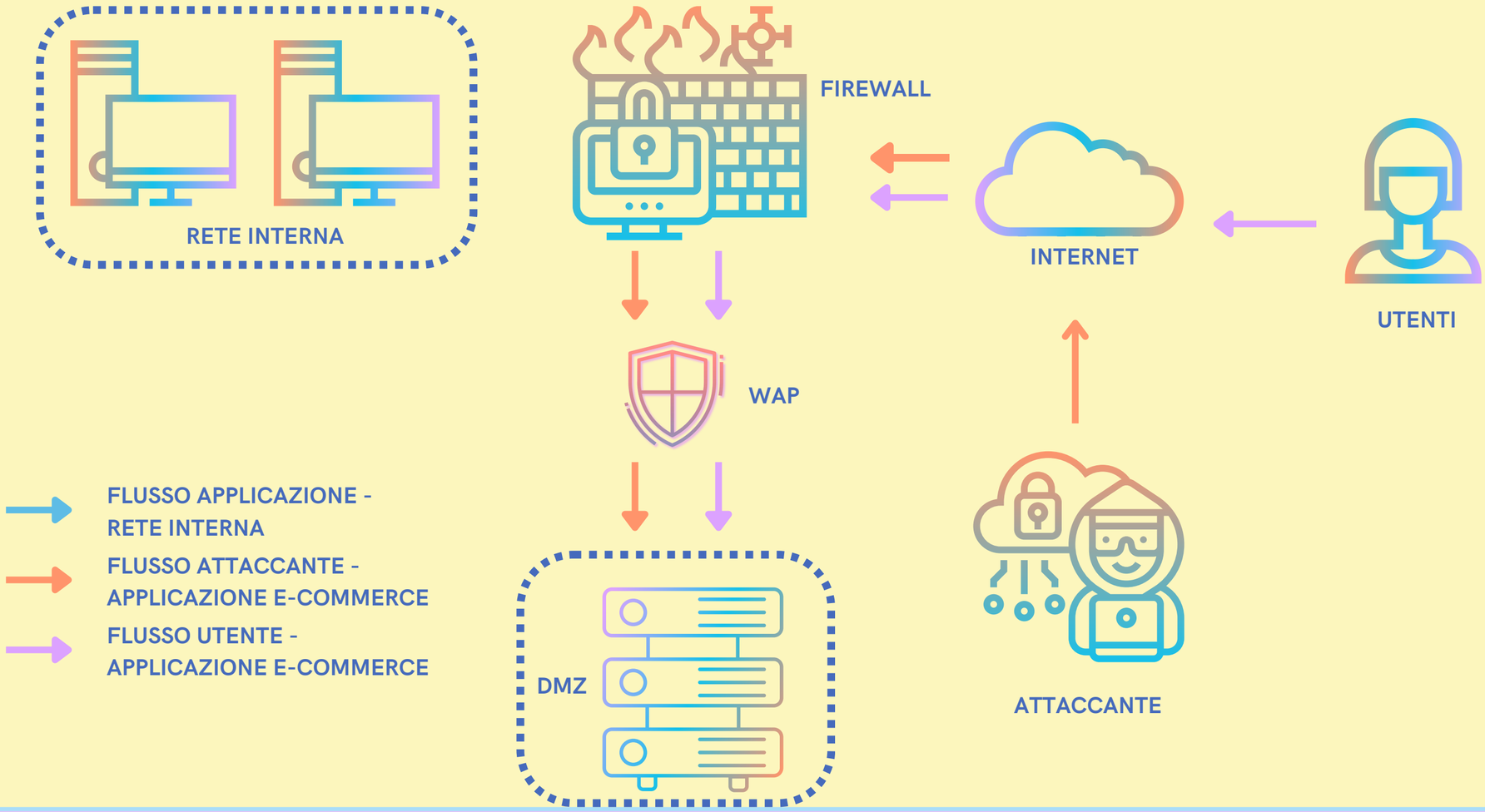


04.Soluzione Completa

Prevenzione SQLi e XSS
Il WAF protegge l'applicazione web filtrando il traffico malizioso.

Isolamento Malware
La regola del firewall che blocca il traffico in uscita dalla DMZ garantisce che eventuali infezioni da malware non si propaghino alla rete interna.

Difesa Stratificata
La combinazione di WAF e firewall protegge applicazione a vari livelli della rete.



05.Modifica più “aggressiva”

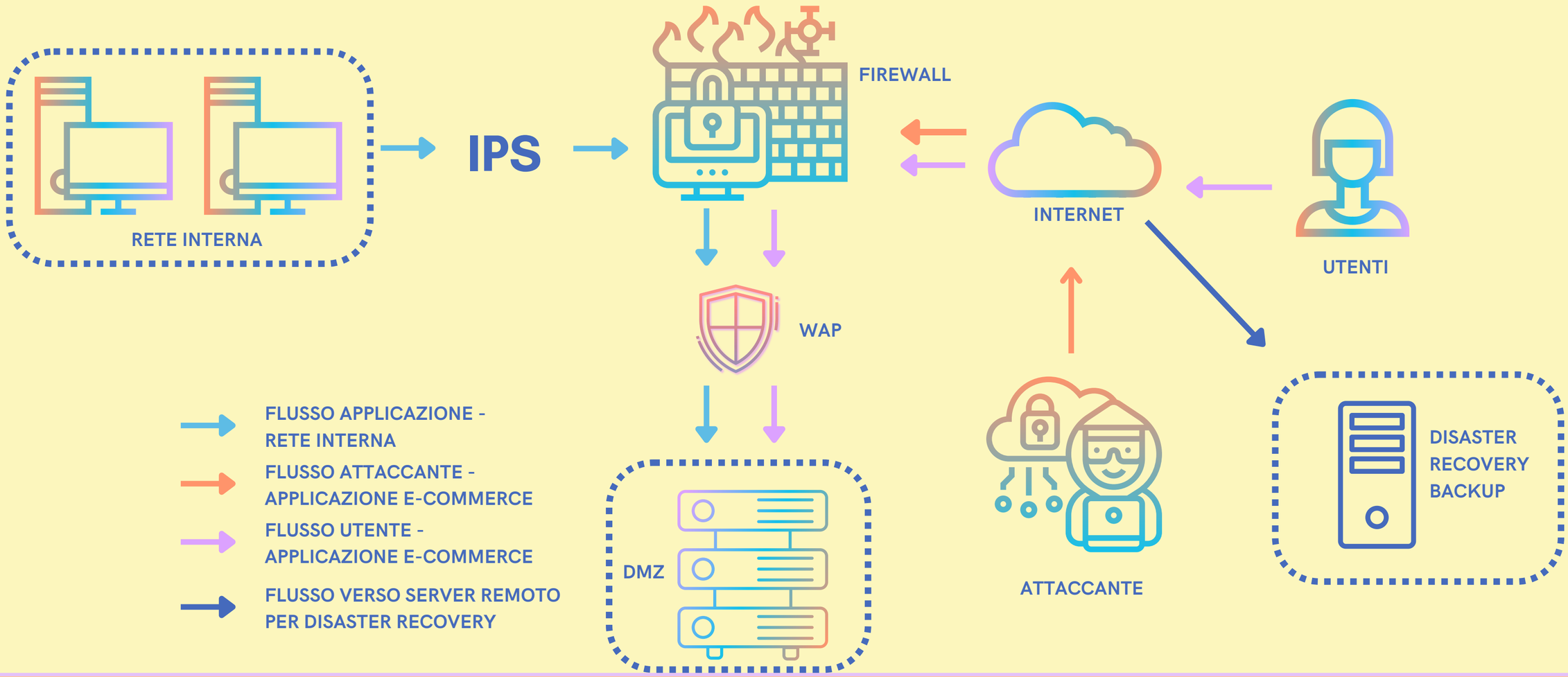
RICHIESTA: fare una modifica piu “aggressiva” dell’infrastruttura, integrando eventuali altri elementi di sicurezza e una soluzione al punto 2. Budget 5000-10000 euro. Eventualmente fare più proposte di spesa.

Per migliorare ulteriormente la sicurezza, possiamo aggiungere misure come IDS/IPS, autenticazione multi-fattore, backup e monitoraggio continuo.

Implementazione di Misure Aggiuntive

- **IDS/IPS (Intrusion Detection/Prevention Systems)**: monitorano e bloccano attività sospette in tempo reale.
- **Autenticazione Multi-Fattore (MFA)**: più forme di **verifica** per accedere ai sistemi, aumentando la sicurezza.
- **Backup e Disaster Recovery**: pianificare e testare regolarmente i backup per garantire la continuità del servizio in caso di attacchi.
- **Monitoraggio Continuo e Risposta agli Incidenti**: implementare soluzioni di monitoraggio per rilevare e rispondere rapidamente agli incidenti.

05.Modifica più “aggressiva”



05.Modifica più “aggressiva”

Per stimare la spesa necessaria per la modifica aggressiva dell'infrastruttura di rete con un budget compreso tra 5000 e 10000 euro, si possono suddividere i costi in diverse categorie.
I costi possono variare a seconda delle specifiche esigenze, delle soluzioni scelte e dei fornitori.
Qui di seguito una stima dettagliata dei costi per le varie implementazioni di sicurezza necessarie.

1. **Web Application Firewall (WAF)**, essenziale per proteggere l'applicazione contro attacchi come SQLi e XSS.
   - Costo stimato: **1000 - 3000 euro** (soluzioni basate su cloud o hardware)
2. **Intrusion Detection/Prevention Systems (IDS/IPS)** per rilevare e prevenire intrusioni e attività sospette.
   - Costo stimato: **1000 - 2000 euro** (soluzioni open source configurate internamente o appliance commerciali)
3. **Autenticazione Multi-Fattore (MFA)** per aggiungere un livello di sicurezza per l'accesso ai sistemi critici.
   - Costo stimato: **500 - 1500 euro** (dipende dal numero di utenti e dalla soluzione scelta)
4. **Segmentazione della Rete** per migliorare la sicurezza isolando le diverse zone della rete.
   - Costo stimato: **500 - 2000 euro** (può includere configurazione di VLANs e ulteriori firewall interni)
5. **Backup e Disaster Recovery** per proteggere i dati aziendali.
   - Costo stimato: **500 - 1000 euro** (soluzioni di backup basate su cloud o hardware dedicato)
6. Servizio di **Mitigazione DDoS**:
   - Costo stimato: **2000 - 4000 euro**

Totale Stimato

- Costo totale stimato: **5500 - 13500 euro**

Il budget totale stimato per le modifiche più aggressive dell'infrastruttura varia **tra 5500 e 13500 euro**, che potrebbe superare leggermente il limite massimo del budget di 10000 euro. Tuttavia, è possibile **rivedere le priorità** e le soluzioni adottate per rispettare il budget previsto, scegliendo **opzioni più economiche o open source quando possibile.**

CONCLUSIONI

L'esercizio ha fornito una comprensione approfondita delle **misure preventive** e delle **azioni di risposta** necessarie per **proteggere un'applicazione web da varie minacce di cybersecurity**.
Si apprende l'importanza di implementare misure preventive come le **query parametrizzate**, la **sanitizzazione** degli **input** e l'utilizzo di un **WAF** per **prevenire attacchi SQLi e XSS**. Inoltre, si è calcolato l'**impatto economico di un attacco DDoS** e discusso le misure preventive per mitigare tali attacchi.
Nella risposta agli incidenti, si evidenzia l'importanza di **isolare le macchine infette** e **segmentare la rete** per contenere la propagazione del malware. L'integrazione delle soluzioni preventive e di risposta ha permesso di sviluppare una strategia completa per la sicurezza dell'applicazione e-commerce.
Infine, sono state esplorate **ulteriori misure di sicurezza** per una protezione più aggressiva dell'infrastruttura, come **l'implementazione** di **IDS/IPS, MFA**, **backup regolari** e **monitoraggio continuo**.
Questo esercizio ha dimostrato **l'importanza** di una **strategia di sicurezza multilivello** e di una **pronta risposta** agli **incidenti** per proteggere le applicazioni web da varie minacce.
Ulteriori passaggi per l'apprendimento potrebbero includere la simulazione di attacchi reali e la revisione regolare delle misure di sicurezza per adattarsi alle nuove minacce emergenti.