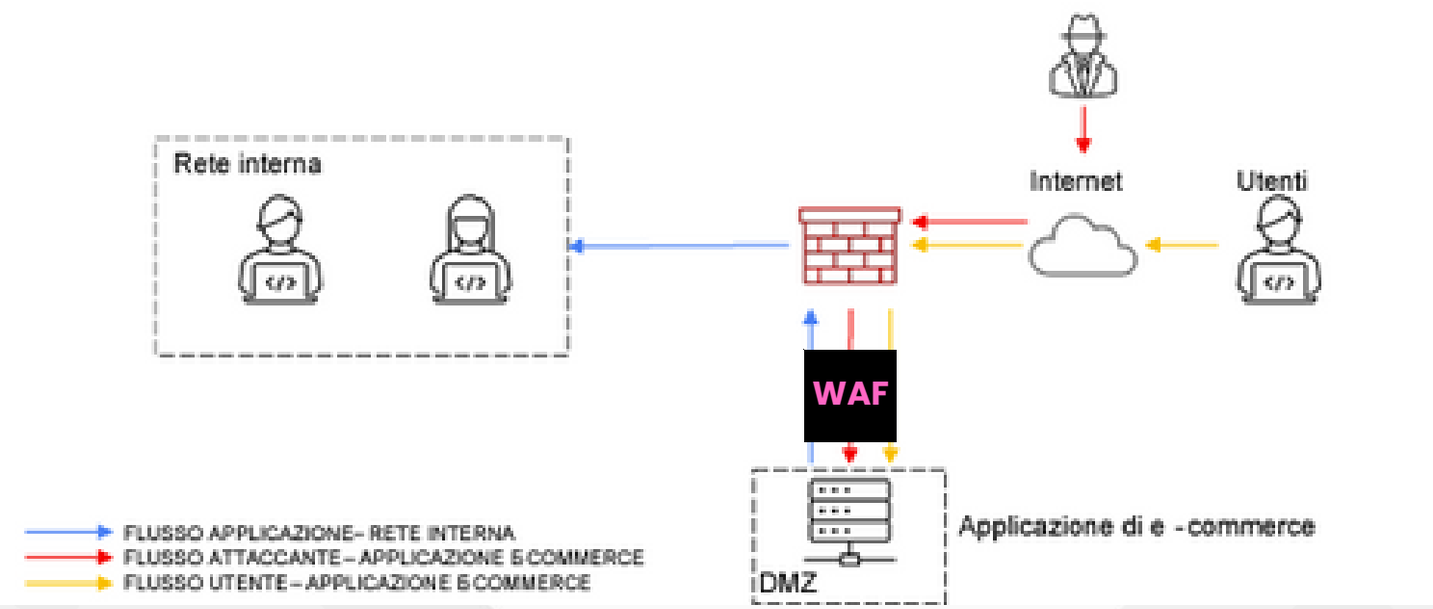
Traccia:

- **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?



Abbiamo usato un **WAF** tra la DMZ e il firewall per proteggere l'applicazione web dagli attacchi SQLi e XSS, filtrare il traffico maligno prima che raggiunga il server nella DMZ, aggiungere livelli di sicurezza oltre al firewall tradizionale, monitorare e registrare tentativi di attacco in tempo reale.

Per difendere l'applicazione web da attacchi SQLi e XSS, ecco alcune azioni preventive che possiamo implementare:

- Web Application Firewall (WAF): Mettiamo un WAF tra la DMZ e il firewall per filtrare e bloccare richieste sospette che potrebbero contenere attacchi SQLi o XSS. Il WAF è fondamentale per proteggere l'applicazione e-commerce da attacchi comuni ma pericolosi.

- Validazione dell'Input: Assicuriamoci che tutti i dati immessi dagli utenti siano corretti e conformi ai formati attesi, sia sul lato server che sul lato client. Questo ci aiuta a prevenire l'inserimento di dati dannosi.

- Sanitizzazione dell'Input: Puliamo i dati forniti dagli utenti rimuovendo o codificando i caratteri pericolosi. Questo passaggio è essenziale per evitare che codice dannoso venga eseguito all'interno dell'applicazione.

- Parametrizzazione delle Query SQL: Utilizziamo query parametrizzate o prepared statements per tutte le interazioni con il database. Questo metodo impedisce agli attaccanti di manipolare le query SQL.

- Encoding dell'Output: Prima di restituire i dati all'utente, applichiamo il corretto encoding. Questo previene l'inserimento di script dannosi nelle pagine web.

- Content Security Policy (CSP): Implementiamo una CSP per limitare le risorse che il browser può caricare ed eseguire. In questo modo, riduciamo il rischio che script non autorizzati vengano eseguiti.

- Aggiornamenti e Patch di Sicurezza: Manteniamo aggiornati tutti i componenti dell'applicazione, inclusi framework e librerie di terze parti, per chiudere eventuali vulnerabilità.

- Monitoraggio e Logging: Implementiamo sistemi di monitoraggio e logging per rilevare e rispondere tempestivamente ai tentativi di attacco. Questi sistemi ci forniscono visibilità sui comportamenti sospetti.

- Implementando queste azioni preventive, possiamo rafforzare significativamente la sicurezza della nostra applicazione web e proteggerla dagli attacchi SQLi e XSS.

Traccia 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 1.200 € sulla piattaforma di e-commerce . Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica

Se l'applicazione web subisce un attacco di tipo DDoS e diventa non raggiungibile per 10 minuti, possiamo calcolare l'impatto finanziario basandoci sulla spesa media degli utenti.

Dati:

Durata dell'interruzione: 10 minuti
Spesa media degli utenti per minuto: 1.200 €
Calcolo dell'Impatto:

Impatto finanziario = Durata dell’interruzione × Spesa media per minuto

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

Quindi, l'impatto finanziario dovuto alla non raggiungibilità del servizio per 10 minuti è di 12.000 €.

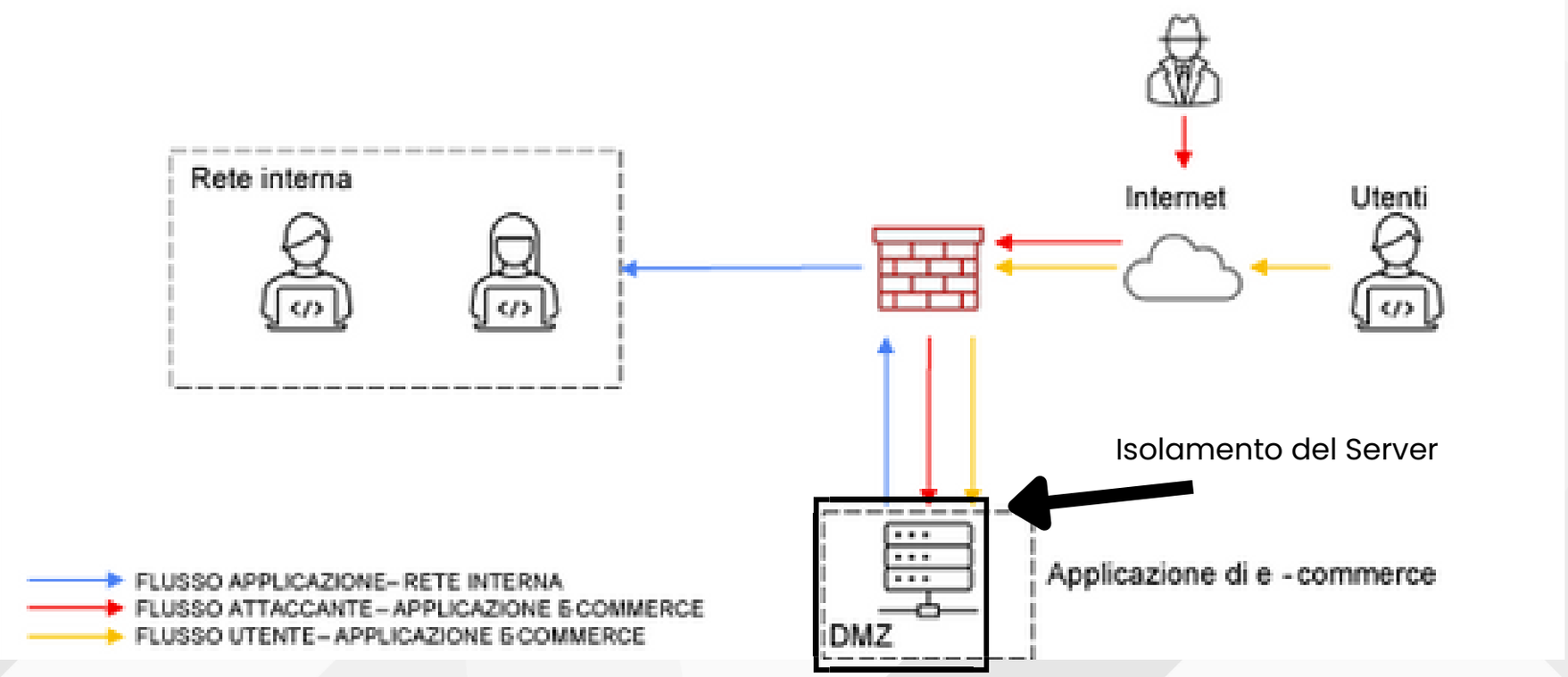
Azioni Preventive Contro gli Attacchi **DDoS**

Per prevenire o mitigare l'impatto di futuri attacchi DDoS, possiamo implementare le seguenti azioni:

- Servizio di Mitigazione DDoS:
- Implementare un servizio di mitigazione DDoS tramite fornitori come Cloudflare, Akamai, o AWS Shield. Questi servizi possono rilevare e filtrare il traffico DDoS prima che raggiunga l'applicazione.
Ridondanza e Bilanciamento del Carico:
- Utilizzare server ridondanti e bilanciamento del carico per distribuire il traffico su più server. Questo può aiutare a gestire picchi di traffico elevato causati da un attacco DDoS.
Scalabilità Automatica:
- Configurare l'infrastruttura per scalare automaticamente in risposta a un aumento del traffico. I servizi cloud offrono opzioni per aggiungere risorse in tempo reale quando necessario.
Monitoraggio e Allarme:
- Implementare sistemi di monitoraggio in tempo reale per rilevare anomalie nel traffico. Configurare allarmi per notificare tempestivamente il personale IT in caso di attacco DDoS.
Rate Limiting e Filtraggio IP:
- Applicare limitazioni di frequenza per le richieste provenienti da singoli indirizzi IP. Bloccare gli IP noti per comportamenti malevoli o sospetti.

Traccia 3:

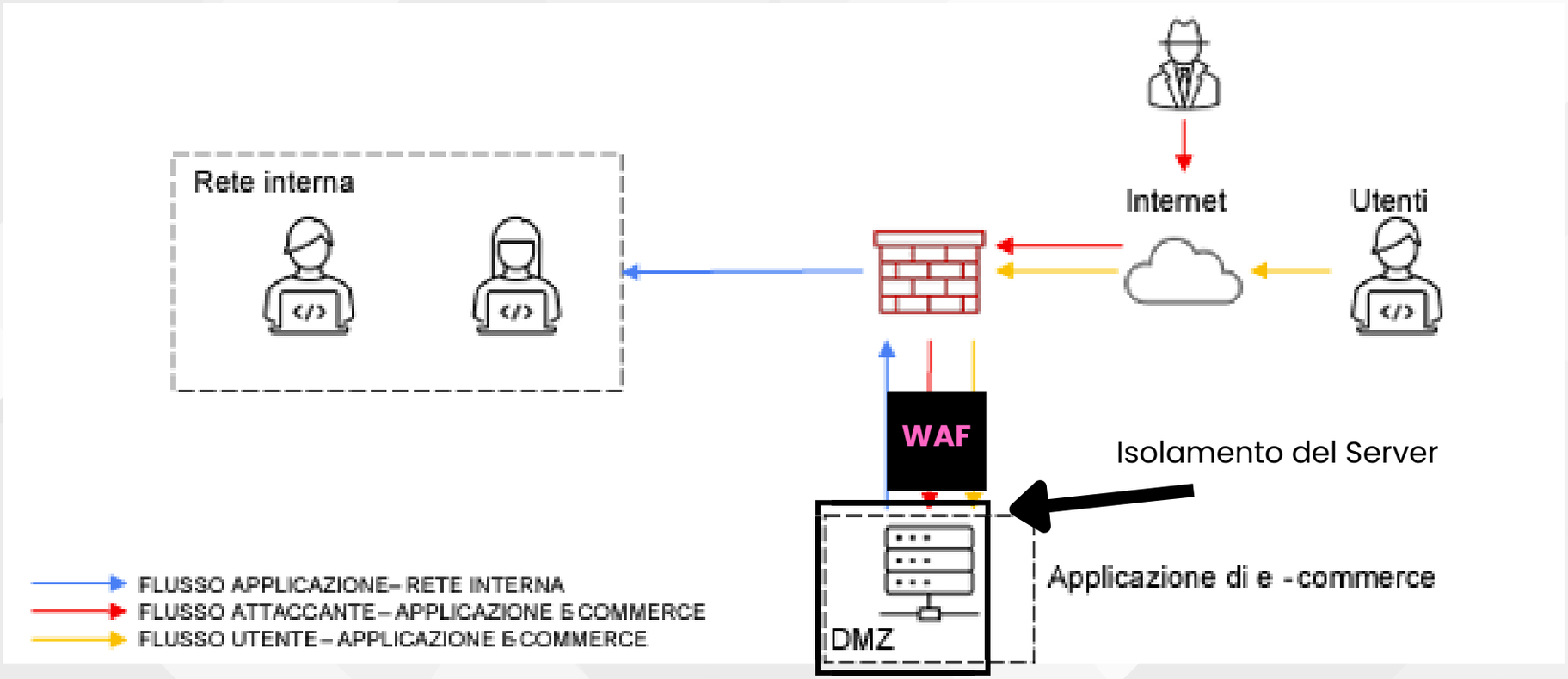
- **Response** : l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura in slide 2 con la soluzione proposta



Abbiamo scelto di isolare il server infetto nella DMZ per una ragione molto semplice: prevenire la propagazione del malware nella nostra rete interna.

Traccia 4:

- **Soluzione completa** : unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)



Traccia 5:

Modifica «più aggressiva» dell'infrastruttura: integrando eventuali altri elementi di sicurezza (integrando anche una soluzione al punto 2) Budget 5000-10000 euro. Eventualmente fare più proposte di spesa

Budget: 10.000 euro

Sistema di Analisi Comportamentale (UBA) — 4000 euro

- Rileva comportamenti anomali degli utenti e delle entità per identificare potenziali minacce interne.

Segmentazione della Rete — 3000 euro

- Divide la rete in segmenti separati per limitare il movimento laterale degli attaccanti.

Autenticazione Multi-Fattore (MFA) — 2000 euro

- Implementa un secondo livello di sicurezza per l'accesso agli account critici.

Formazione sulla Sicurezza per il Personale — 1000 euro

- La formazione sulla sicurezza dovrebbe essere erogata a tutto il personale dell'organizzazione, con un focus particolare su coloro che gestiscono sistemi critici o sensibili.

Implementazione delle misure di sicurezza trovate: