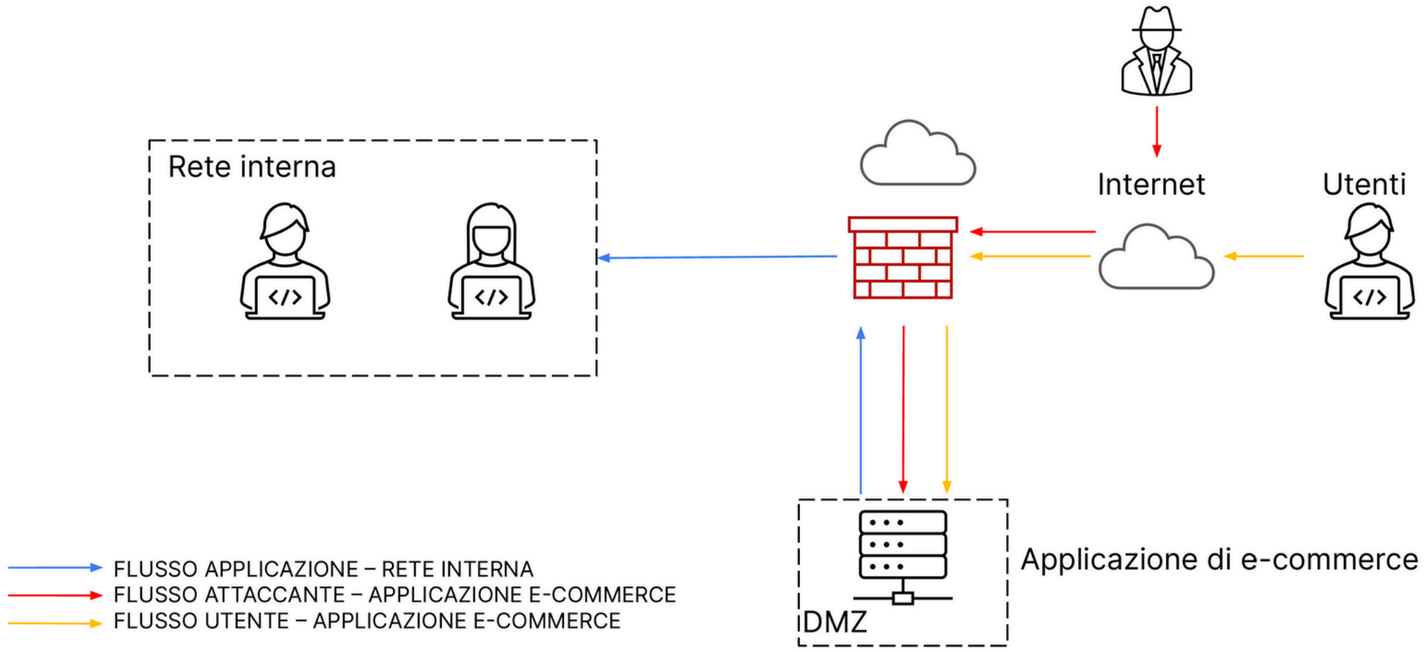
Modulo 5
Esercizio pratico

INDICE

0: introduzione infrastruttura

Architettura di rete:
L'applicazione di e-commerce deve essere disponibile per gli utenti tramite Internet per effettuare acquisti sulla piattaforma.

La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.



Torna al Programma

0: introduzione infrastruttura

- L'infrastruttura è progettata per supportare un'applicazione di e-commerce accessibile agli utenti tramite Internet.

- La rete interna è protetta dalla DMZ tramite politiche di firewall, ma è necessario rivedere le misure di sicurezza per mitigare rischi come attacchi SQLi, XSS, DDoS e malware.

Torna al Programma

1. Prevenzione di attacchi injection (SQLi/XSS)

1. Prevenzione di attacchi injection (SQLi/XSS):

Cosa sono gli attacchi SQLi/XSS

Gli attacchi SQLi (Injection SQL) e XSS (Cross-Site Scripting) sono tecniche per inserire codice malevolo nelle applicazioni Web, compromettendo i dati degli utenti o l'integrità del sistema.

Torna al Programma

1. Prevenzione di attacchi injection (SQLi/XSS):

Prevenzione

- **Implementazione di Web Application Firewall (WAF):** miglior modo per prevenire qualsiasi tipo di attacco alle Web App è di implementare un WAF che monitora il traffico e limita le richieste inviate alle applicazioni.
- **Validazione e sanitizzazione dei dati di input:**

Verificare e "pulire" ogni dato inserito dagli utenti per evitare l'iniezione di codice SQL o script malevoli.

- **Escape delle stringhe di output:**

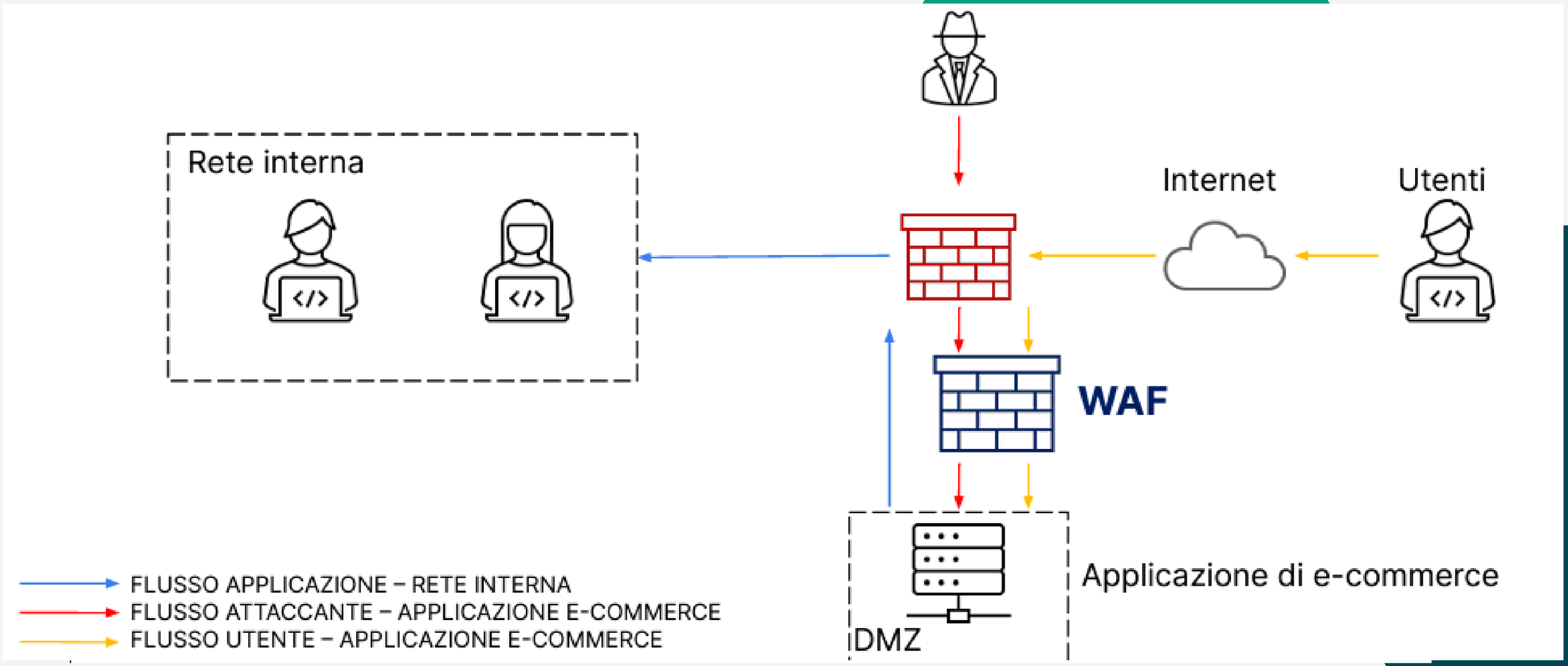
Prima di visualizzare dati forniti dagli utenti sulle pagine web, assicurarsi che siano correttamente "escaped" per prevenire XSS.

- **Aggiornamento regolare dei software:**

Mantenere aggiornati software e framework per proteggere l'applicazione da vulnerabilità conosciute.

Torna al Programma

1: aggiornamento infrastruttura



Torna al Programma

2. Prevenzione attacchi DDoS (Distributed Denial of Service)

Torna al Programma

2. Prevenzione attacchi DDoS:

Indicatore di compromissione e impatto dell'incidente

Torna al Programma

e-commerce non raggiungibile per 10 minuti

Un attacco DDoS rende l'applicazione e-commerce non raggiungibile per 10 minuti.

1.500 euro al minuto Perdita di 15.000 euro

Considerando una spesa media degli utenti di 1.500 € al minuto, l'impatto sull'attività potrebbe essere significativo, con una perdita di 15.000 €.

2. Prevenzione attacchi DDoS:

Indicatore di compromissione e impatto dell'incidente

Torna al Programma

- un attacco DDoS è un attacco coordinato dove numerose macchine (gestite in genere da un master remoto) inviano contemporaneamente grandi quantità di pacchetti allo stesso indirizzo IP, **generando una enorme quantità di traffico.** L'obiettivo è **intasare la rete** ed impedire il corretto funzionamento del servizio.

- l'attacco è riuscito ad impedire il corretto funzionamento per 10 minuti. Sappiamo anche che gli utenti spendono in media 1500 € al minuto.
- **Danno finale:** 1.500 x 10 = 15.000 €

2. Prevenzione attacchi DDoS:

RIP e fase Post-incident, azioni preventive applicabili

- **Usare il WAF** implementato prima per filtrare e gestire il traffico HTTP/HTTPS, proteggendo l'applicazione da attacchi DDoS.
- **Monitoraggio del traffico di rete:** Rilevare e rispondere tempestivamente agli attacchi DDoS con sistemi di monitoraggio avanzati.
- **Capacità di mitigazione:** Aumentare la capacità dei server e distribuire il traffico per resistere agli attacchi DDoS.

Torna al Programma

3. Response: mitigazione di un malware

Torna al Programma

3. Response: mitigazione di un malware

Mitigazione

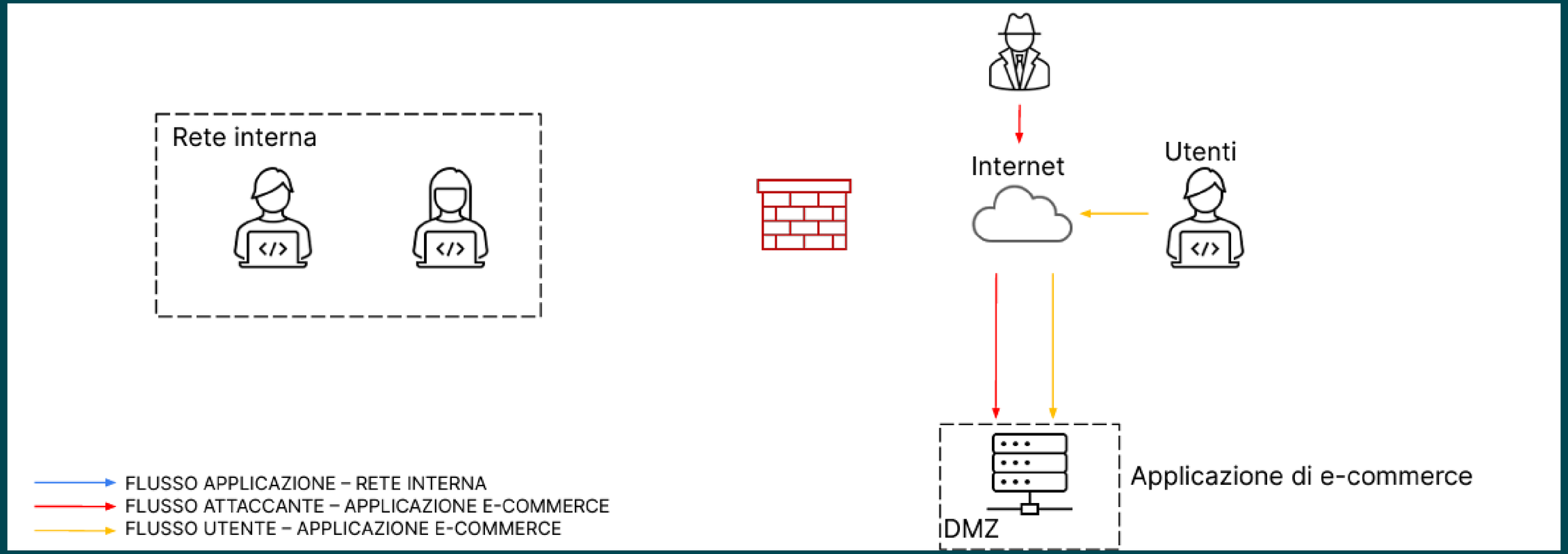
- **Isolamento della macchina infetta:** prevenire propagazione del malware sulla rete attraverso la segmentazione di rete e firewall per isolare la macchina infetta. La macchina rimarrà connessa ad internet ma non sarà consentito alcun movimento sulla rete.

- **Monitoraggio del traffico:** Monitorare attentamente il traffico di rete per rilevare eventuali attività sospette correlate al malware.

- **Scansione antivirus e pulizia:** Eseguire scansioni antivirus e antimalware per individuare e rimuovere il malware dalla macchina infetta.

Torna al Programma

4. Posizione finale dell'azienda: Overview aggiornata dell'infrastruttura



Torna al Programma

CONCLUSIONE

L'azienda deve garantire un'architettura di rete sicura che protegga sia l'applicazione Web accessibile agli utenti esterni tramite la DMZ, sia la rete interna. Revisioni regolari delle politiche di sicurezza, aggiornamenti software, formazione del personale e implementazione di strumenti di monitoraggio sono essenziali per mitigare rischi e proteggere le operazioni aziendali.