PROGETTO

S9/L5

di Giuseppe Lupoi

INDICE

TRACCIA

Con riferimento alla figura in slide 2, rispondere ai seguenti quesiti.

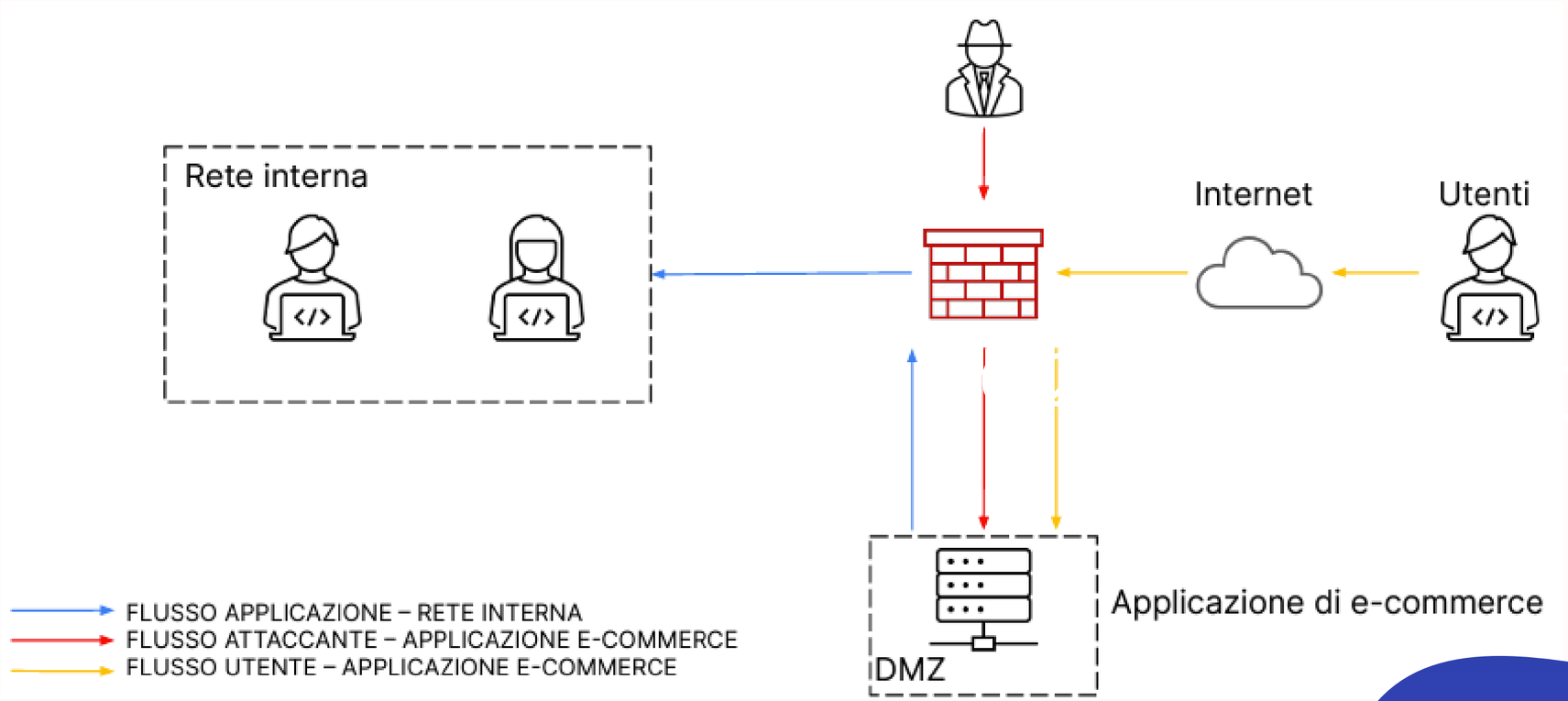
1. Azioni preventive: quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni

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.

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.

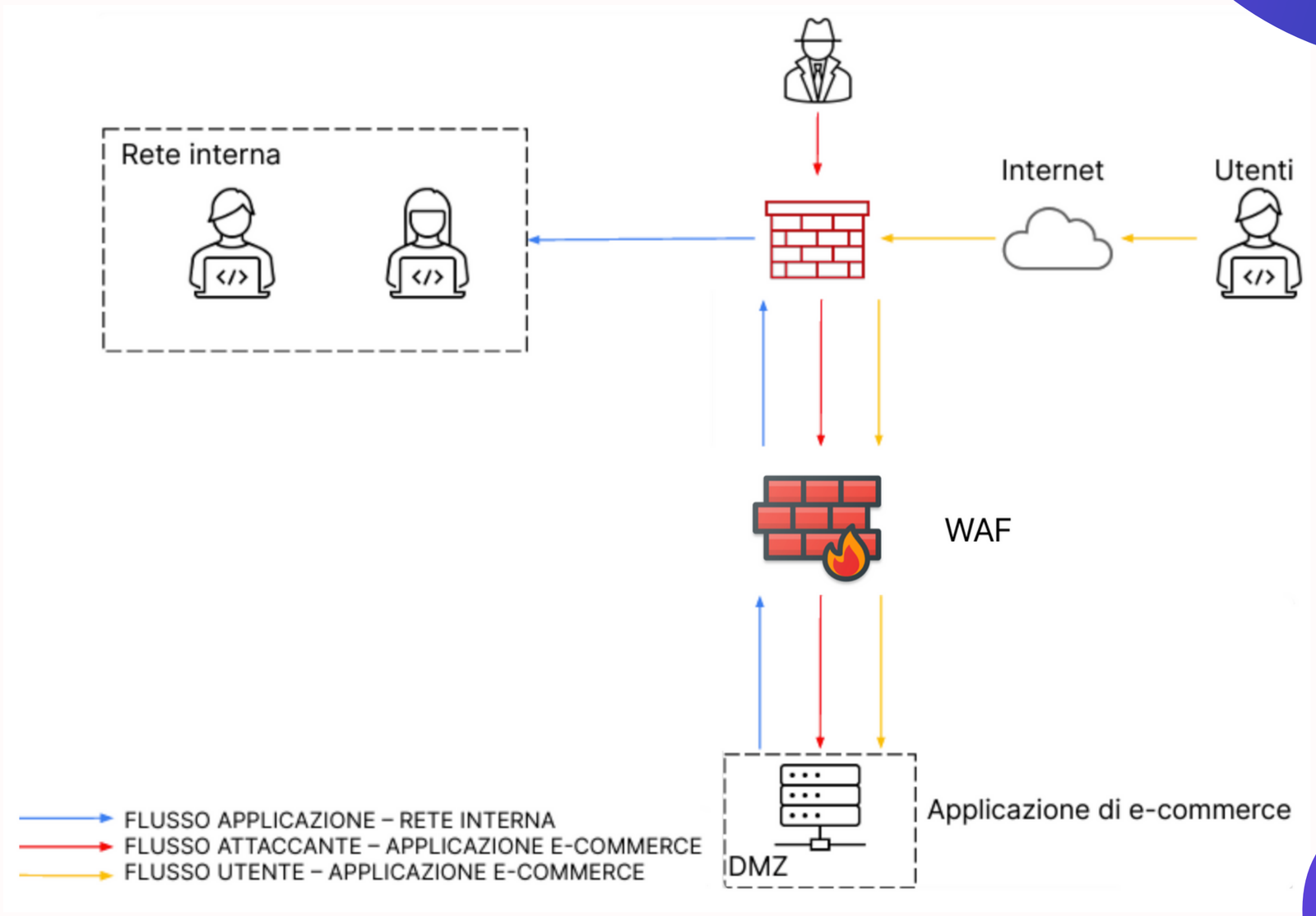


AZIONI PREVENTIVE

Per la risoluzione del primo punto dell'esercitazione di oggi, si potrà procedere con l'aggiunta di un **Web Application Firewall** sistemato a protezione dell'Applicazione di e-commerce dell'azienda.

Si posizionerà quindi nella nuova architettura di rete in aggiunta al firewall già esistente a protezione delle comunicazioni in entrata da utenti e malintenzionati.

Espongo di seguito la nuova architettura di rete:



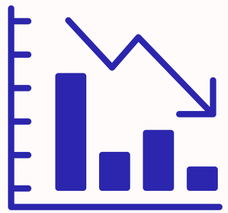
IMPATTI SUL BUSINESS

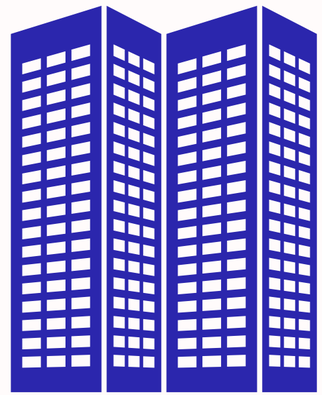
Riguardo il secondo punto della traccia ci viene esposto uno scenario dove l'**applicazione Web** dell'azienda viene colpita da un **attacco Ddos**, perciò l'applicazione rimarrà indisponibile per **10 minuti**. Ci viene chiesto di calcolare l'impatto finanziario sul business considerando che gli **utenti spendono in media 1.500€ al minuto**.

Procedo col calcolo di seguito.
Conoscendo quindi questi dati:
Tempo di inattività dell'applicazione, che chiamerò DT (downtime) = **10min**
Incassi medi in 1 min, che chiamerò LpM (loss per minute) = **1.500€**

Calcolo la perdita totale nel DT, che chiamerò TL (total loss) quindi:

LpM x DT = TL
1.500 x 10 = 15.000€





Si evince quindi da questo calcolo che la perdita totale del nostro business per il tempo di inattività sarà di 15.000€.

RESPONSE

Arrivati al terzo punto della traccia di oggi affronteremo la casistica in cui la nostra Web App venga colpita da un malware.

Ci viene proposto quindi di estraniare la macchina infetta della nostra rete interna, mentre in questo caso non prenderemo in considerazione la rimozione dell'accesso alla macchina da parte dell'attaccante.
Utilizzerò quindi la tecnica dell'**Isolamento** appresa in questa settimana per ovviare al problema suddetto.

Propongo quindi la nuova architettura di rete nella prossima slide.

Espongo di seguito la nuova architettura di rete: