

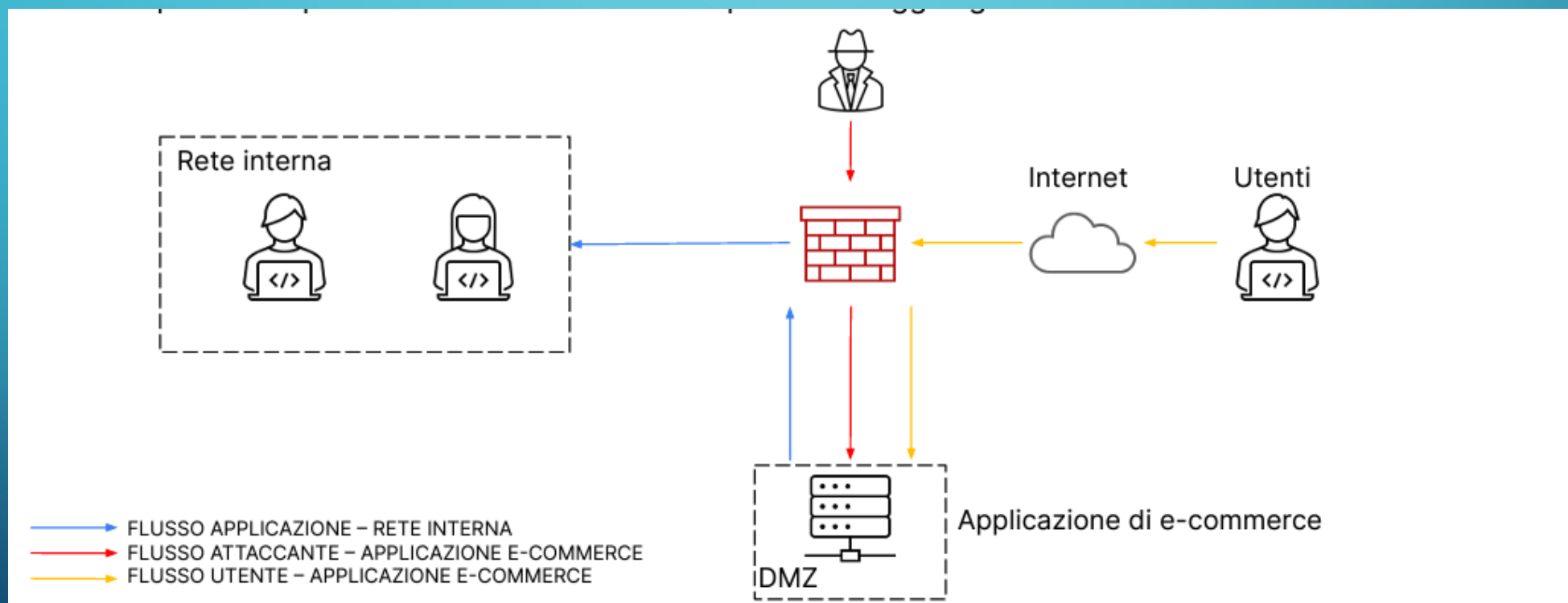


S9L5

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 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.



## IMPATTO SUL BUSINESS

Per calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio a causa di un attacco DDoS, consideriamo i seguenti punti:

Durata dell'indisponibilità del servizio: 10 minuti  
guadagno medio per minuto per gli utenti sulla piattaforma di e-commerce: 1.500 €  
quindi, per calcolare l'impatto totale sull'attività commerciale, moltiplichiamo la durata dell'indisponibilità del servizio per il guadagno medio per minuto per gli utenti:

$\text{Impatto} = \text{Durata indisponibilità del servizio (minuti)} * \text{guadagno medio per minuto per utente}$

$\text{Impatto} = 10 \text{ minuti} * 1.500 \text{ €/minuto}$

$\text{Impatto} = 15.000 \text{ €}$

Quindi, l'impatto sull'attività commerciale dovuto alla non raggiungibilità del servizio per 10 minuti è di 15.000 €.



## RESPONSE

CONSIDERATA L'EMERGENZA, SI PUÒ ADOTTARE UNA STRATEGIA BASATA SULL'ISOLAMENTO DELLA MACCHINA INFETTATA. IN QUESTO CASO LA MACCHINA SARÀ DIRETTAMENTE COLLEGATA AD INTERNET, RAGGIUNGIBILE DALL'ATTACCANTE MA NON PIÙ CONNESSA ALLA RETE INTERNA. LA FIGURA SLIDE MOSTRA LA STRATEGIA DELL'ISOLAMENTO DELLA MACCHINA INFETTA. DA NOTARE COME NON CI SIA PIÙ COMUNICAZIONE TRA L'APPLICAZIONE WEB E LA RETE INTERNA.

