S9-LS5

ANALISI DEI LOG

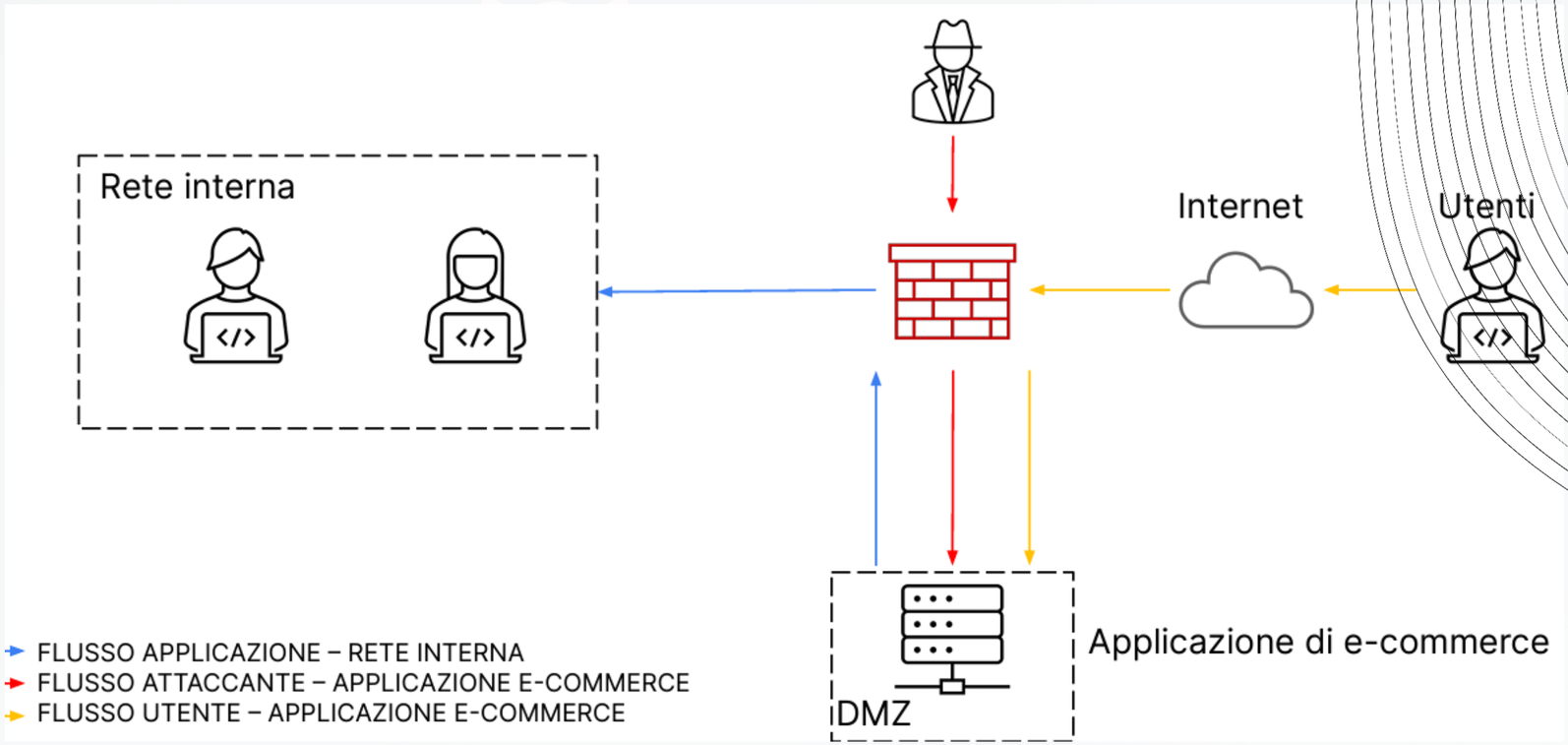
INDICE

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

SCHEMA DI RETE - BASE



SOLUZIONE SQL INJECTION

PER PREVENIRE ATTACCHI DI TIPO SQL INJECTION (SQLI) E CROSS-SITE SCRIPTING (XSS), È FONDAMENTALE COMPRENDERE LE LORO CAUSE. LE SQL INJECTION SI VERIFICANO QUANDO INPUT DI TESTO VENGONO INTERPRETATI ERRONEAMENTE DAL DATABASE, CHE LI CONSIDERA COME QUERY INTERNE PASSATE IN MODO MALEVOLO COME INPUT DI TESTO. L'OBIETTIVO DI TALI ATTACCHI È RECUPERARE O BYPASSARE I SISTEMI DI DIFESA DEL DATABASE.

LE SQL INJECTION POSSONO SFRUTTARE LA MANCATA SANITIZZAZIONE DEI DATI DI INPUT, CONSENTENDO L'INSERIMENTO DI COMANDI SQL DANNOSI. PER PREVENIRE QUESTO TIPO DI ATTACCO, È ESSENZIALE UTILIZZARE QUERY PARAMETRICHE O DICHIARAZIONI PREPARATE, CHE SEPARANO I DATI DAGLI STATEMENT SQL E IMPEDISCONO L'ESECUZIONE NON DESIDERATA DI COMANDI.

SOLUZIONE XSS

D'ALTRA PARTE, GLI ATTACCHI DI TIPO XSS SI VERIFICANO QUANDO I DATI DI INPUT DEGLI UTENTI VENGONO INSERITI NELLE PAGINE WEB SENZA LA CORRETTA SANITIZZAZIONE, PERMETTENDO L'ESECUZIONE DI SCRIPT DANNOSI LATO CLIENT. PER ELIMINARE QUESTO RISCHIO, È NECESSARIO SANITIZZARE I DATI PRIMA DI INVIARLI AL DB PER POI FARLI VISUALIZZARE NELLE PAGINE HTML, IMPEDENDO L’ESECUZIONE E IL SALVATAGGIO DI SCRIPT MALEVOLI.

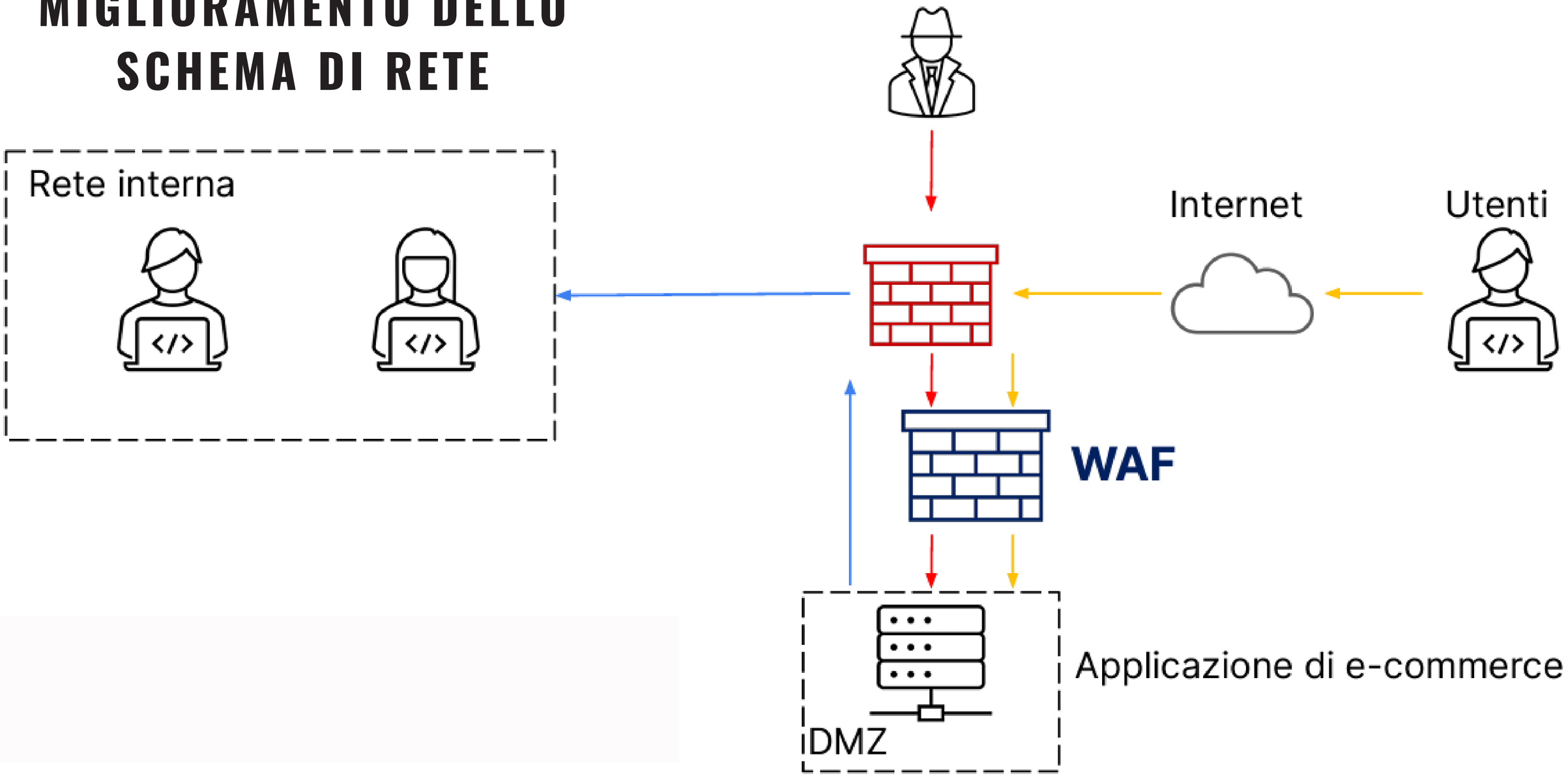
FIREWALL WAF

IL WEB APPLICATION FIREWALL , È UN TIPO SPECIFICO DI FIREWALL PROGETTATO PER PROTEGGERE LE APPLICAZIONI WEB DA UNA VARIETÀ DI MINACCE. A DIFFERENZA DEI FIREWALL TRADIZIONALI, CHE SI CONCENTRANO PRINCIPALMENTE SUL CONTROLLO DEL TRAFFICO DI RETE BASATO SU INDIRIZZI IP E PORTE, IL WAF OPERA A UN LIVELLO PIÙ ALTO, FOCALIZZANDOSI SULLA SICUREZZA DELLE APPLICAZIONI WEB

UN WAF ANALIZZA LE RICHIESTE HTTP IN ARRIVO PER RILEVARE PATTERN SOSPETTI O ATTACCHI NOTI, COME TENTATIVI DI SQL INJECTION, XSS E ALTRI TIPI DI VULNERABILITÀ WEB

ALCUNI WAF UTILIZZANO ANALISI COMPORTAMENTALE PER IDENTIFICARE MODELLI ANOMALI O COMPORTAMENTI SOSPETTI ALL'INTERNO DEL TRAFFICO WEB. QUESTO APPROCCIO PUÒ ESSERE EFFICACE NEL RILEVARE ATTACCHI CHE NON SEGUONO SCHEMI PREDEFINITI

MIGLIORAMENTO DELLO SCHEMA DI RETE



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

STIMA PERDITA ECONOMICA

CALCOLO DELL'IMPATTO FINANZIARIO:IMPATTO SUL BUSINESS=SPESA MEDIA DEGLI UTENTI AL MINUTO×DURATA DELL’INDISPONIBILITA`IMPATTO SUL BUSINESS=SPESA MEDIA DEGLI UTENTI AL MINUTO×DURATA DELL’INDISPONIBILITA`

IMPATTO SUL BUSINESS=1.500€×10 MINUTI=15.000€

PERTANTO, L'IMPATTO FINANZIARIO A CAUSA DEI 10 MINUTI DI INDISPONIBILITÀ DELLA PIATTAFORMA DI E-COMMERCE È DI 15.000 €. QUESTO VALORE RAPPRESENTA LA STIMA DEL MANCATO GUADAGNO POTENZIALE DURANTE IL PERIODO DI NON RAGGIUNGIBILITÀ DEL SERVIZIO.

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 con le evidenze delle implementazioni.

RISPOSTA ALL'ATTACCO

PER PREVENIRE ULTERIORI DANNI CAUSATI DAL MALWARE E MONITORARE ATTENTAMENTE LE AZIONI DELL'ATTACCANTE, POSSIAMO AGIRE NEL SEGUENTE MODO:

SCOLLEGAMENTO DALLA RETE INTERNA: LA MACCHINA INFETTA SARÀ DISCONNESSA DALLA RETE INTERNA PER PREVENIRE IL FURTO DI DATI E LA PROPAGAZIONE DEL MALWARE TRA LE ALTRE MACCHINE AZIENDALI.

POSIZIONAMENTO IN RETE DI QUARANTENA SU INTERNET: LA MACCHINA SARÀ POSIZIONATA SU UNA RETE DI QUARANTENA SU INTERNET, MANTENENDO L'ACCESSIBILITÀ ALL'ATTACCANTE MA LIMITANDONE L'IMPATTO. QUESTA CONFIGURAZIONE CONSENTE DI OSSERVARE LE ATTIVITÀ DELL'ATTACCANTE IN UN AMBIENTE SICURO.

MONITORAGGIO DELLE ATTIVITÀ: SARÀ IMPLEMENTATO UN MONITORAGGIO COSTANTE PER REGISTRARE OGNI MOVIMENTO DELL'ATTACCANTE SULLA MACCHINA INFETTA. QUESTO INCLUDE LA RILEVAZIONE DI COMPORTAMENTI SOSPETTI O TENTATIVI DI ULTERIORE ATTACCHI.

ANALISI FORENSE: DURANTE IL PERIODO DI QUARANTENA, SARANNO EFFETTUATE ANALISI FORENSI PER COMPRENDERE LA NATURA DELL'ATTACCO, IDENTIFICARE LE VULNERABILITÀ SFRUTTATE E RACCOGLIERE PROVE UTILI PER AZIONI LEGALI O MITIGAZIONI FUTURE.

MIGLIORAMENTO DELLO SCHEMA DI RETE