

S9L5

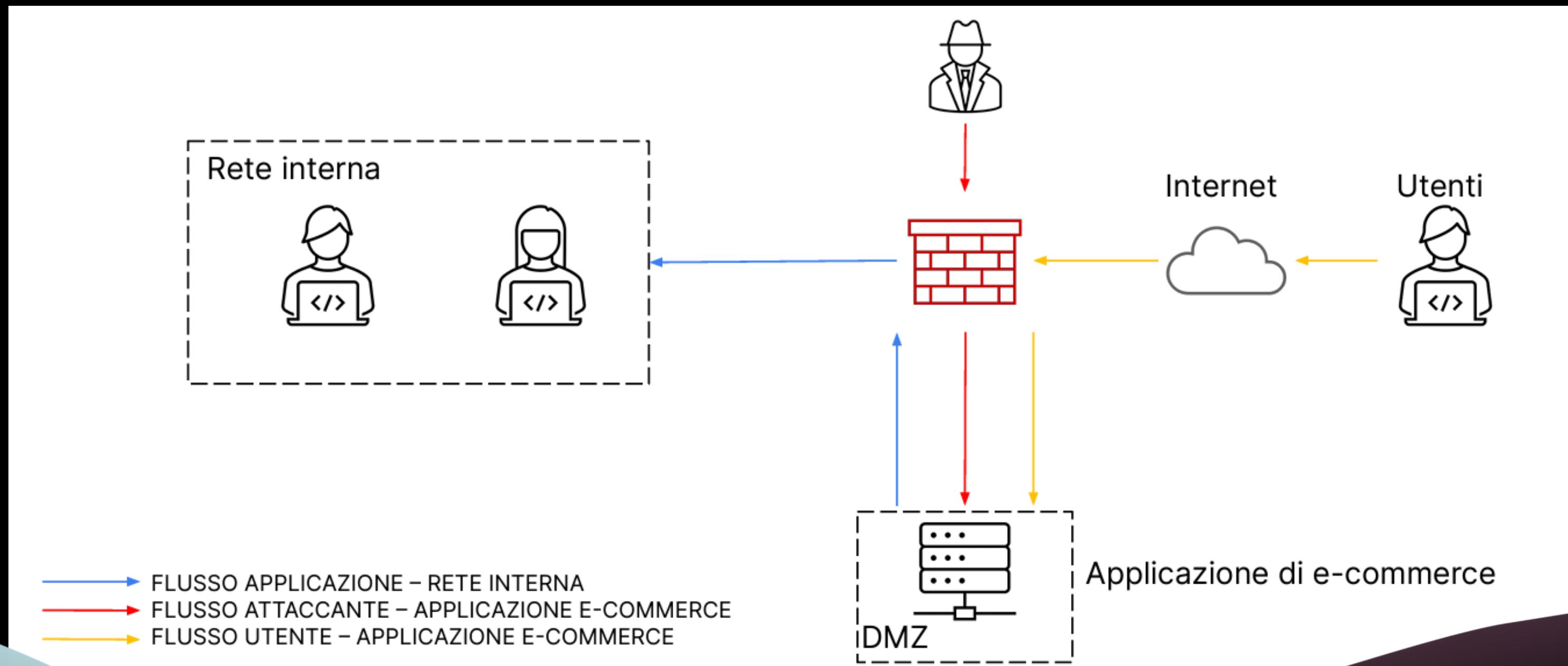
Prevenzione e response di una rete

- ARCHITETTURA DI RETE
- AZIONI PREVENTIVE
- IMPATTI SUL BUSINESS
- RESPONSE

INDICE

ARCHITETTURA DI RETE

L'architettura in questione consiste in una rete interna, un firewall e una applicazione di e-commerce



CONFIGURAZIONE

- La rete interna è raggiungibile dalla DMZ dell'app e-commerce, ma non può connettersi a internet
- L'applicazione di e-commerce è disponibile per gli utenti tramite internet per effettuare acquisti sulla piattaforma.

RISCHI

- Un malintenzionato tramite rete internet può attaccare la DMZ, comprometterla, e per via delle regole firewall accedere alla rete interna

AZIONI PREVENTIVE

quali azioni preventive sono implementabili per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato?

Utilizzo di WAF (Web Application Firewall):

- Implementare un WAF per filtrare e bloccare attacchi XSS e SQLi a livello di rete, proteggendo la Web App da input malevoli provenienti da malintenzionati.

Validazione e Sanitizzazione degli Input:

- Validare e sanificare rigorosamente tutti gli input utente, filtrando caratteri speciali, codice e queries potenzialmente dannose.

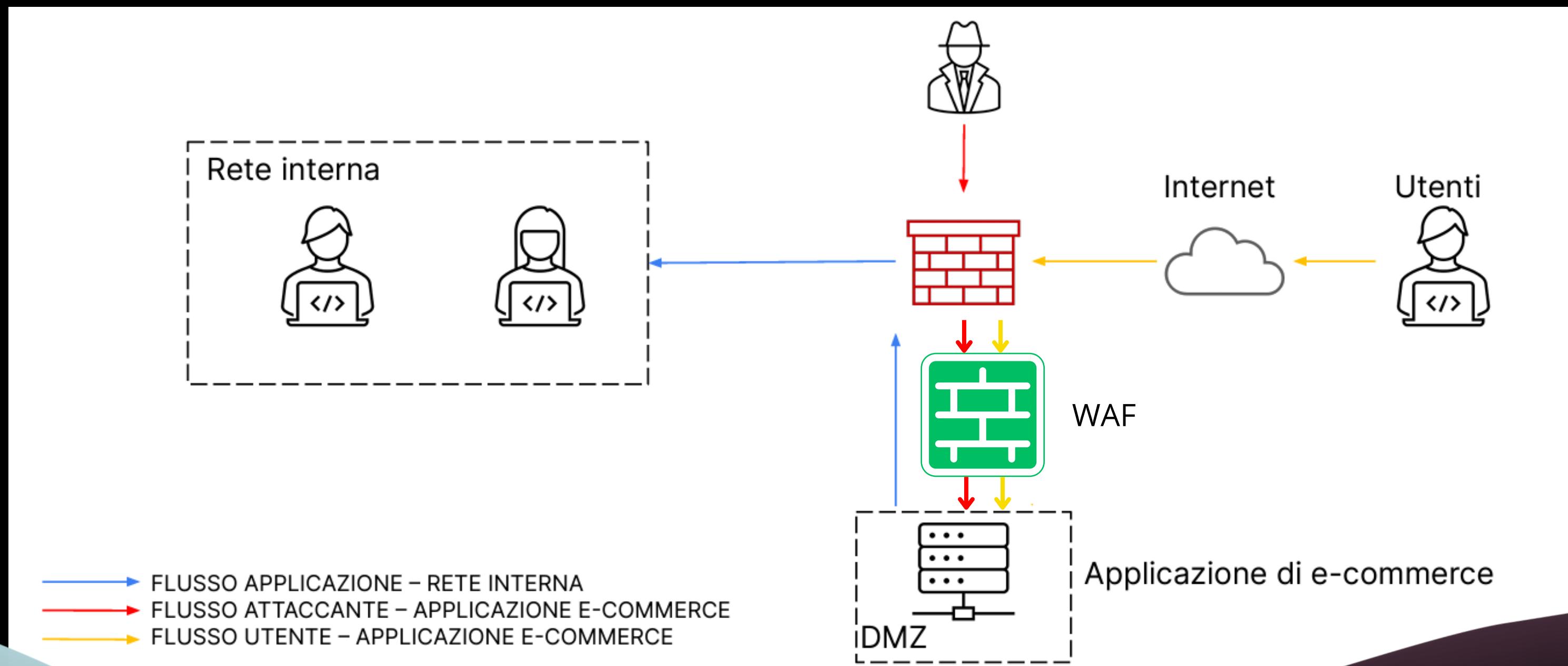
APPROFONDIMENTO: WAF

Un WAF, acronimo di Web Application Firewall, è un'applicazione o un dispositivo che fornisce una protezione aggiuntiva alle applicazioni web contro una serie di minacce e attacchi online.

Il suo scopo principale è filtrare, monitorare e bloccare il traffico HTTP proveniente o diretto a un'applicazione web, al fine di proteggere l'applicazione da vulnerabilità e attacchi come Cross-Site Scripting (XSS), Injection SQL, e altre forme di exploit che mirano alle debolezze delle applicazioni web.

MODIFICA ALLA RETE

L'architettura in questione consiste in una rete interna, un firewall, un WAF e una applicazione di e-commerce



IMPATTI SUL BUSINESS

l'applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione non raggiungibile per 10 minuti.

Ogni minuto gli utenti spendono circa 1.500 € sulla piattaforma.

Stima dei danni

- I danni causati dal mancato guadagno sul business possono essere stimati moltiplicando la spesa potenziale degli utenti, fissata a 1.500€ al minuto, per la durata dell'indisponibilità del servizio, che è stata di 10 minuti.

Risultati

- per 10 minuti di indisponibilità la compagnia ha perso 15.000 € di acquisti potenziali.

RESPONSE

L'applicazione Web viene infettata da un malware.

La nostra priorità è che il malware non si propaghi nella rete interna, senza rimuovere l'accesso da parte dell'attaccante alla macchina infettata.

Isolamento

- Considerando l'urgenza della situazione, è possibile implementare una strategia incentrata sull'isolamento della macchina infettata. In tale contesto, la macchina sarà direttamente connessa a Internet, accessibile all'attaccante, ma non avrà più accesso alla rete interna.

Motivazione

- Permettendo all'attaccante di poter accedere alla web app è possibile studiare come è stato eseguito l'attacco, per poi formulare una risposta e un metodo per evitare che capiti nuovamente, evitando nel frattempo che il malintenzionato possa accedere alla rete interna.

APPROFONDIMENTO: ISOLAMENTO

L'isolamento è una strategia di sicurezza che prevede separare una macchina compromessa o dalla rete, al fine di prevenire la diffusione di malware, la compromissione di altri dispositivi e il danneggiamento dell'intera rete.

- **Separazione dalla Rete Interna:** La macchina compromessa viene disconnessa dalla rete interna dell'organizzazione. Questo impedisce al malware di propagarsi e compromettere altri sistemi.
- **Connessione Diretta ad Internet:** Se necessario per scopi di analisi e monitoraggio, la macchina infetta può essere mantenuta connessa a Internet, consentendo agli amministratori di sistema di raccogliere informazioni sulla minaccia e applicare patch.
- **Analisi Forense:** L'isolamento fornisce un ambiente controllato per condurre un'analisi forense sulla macchina infetta. Gli esperti di sicurezza possono esaminare il sistema senza il rischio di ulteriori compromissioni.
- **Limitazione del Danno:** L'isolamento mira a limitare il danno causato da un'eventuale infezione, riducendo al minimo l'impatto sui sistemi circostanti e proteggendo i dati sensibili.

MODIFICA ALLA RETE

Notare come non ci sia più collegamento tra la web app e la rete interna.

