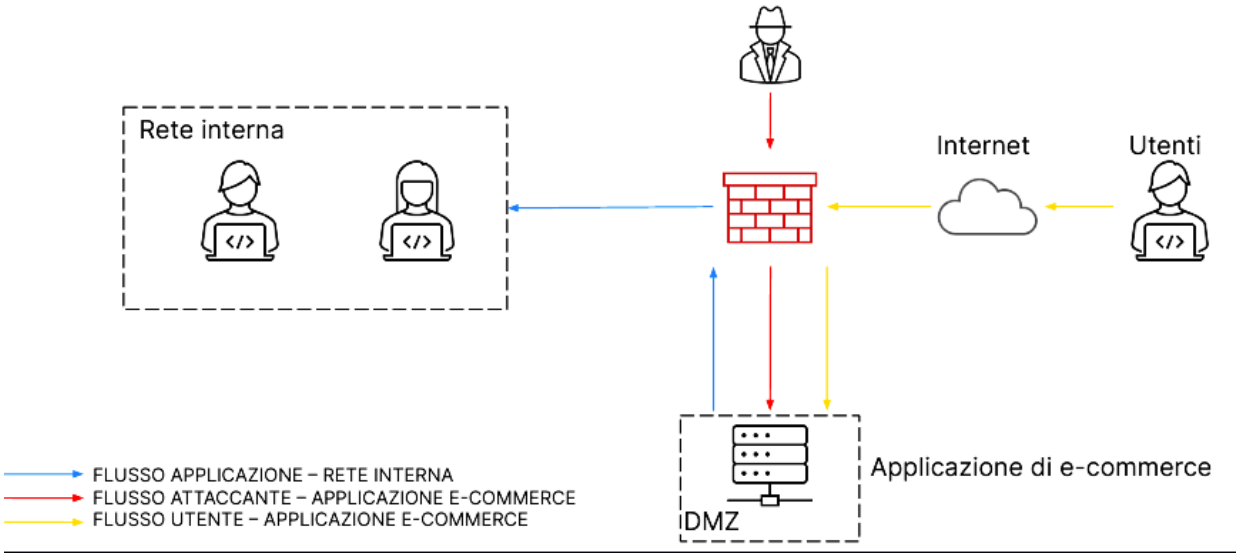
Progetto S9/L5: Analisi dei log

Nella Traccia troviamo la seguente architettura di rete.



- **Requisiti 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.

Procediamo quindi a risolvere i vari quesiti richiesti

- **Azioni preventive:**
  Per proteggere l'applicazione Web da attacchi di tipo SQLi o XSS da parte di utenti malintenzionati, stiamo introducendo misure preventive. Modificheremo la figura della rete fornita per evidenziare queste implementazioni.

- **Impatti sul business:**
  Valutiamo l'impatto commerciale causato dalla temporanea indisponibilità dell'applicazione Web a causa di un attacco DDoS esterno, che ha reso il servizio inaccessibile per un periodo di 10 minuti. Questa valutazione tiene conto del fatto che, in media, gli utenti spendono 1.500 € al minuto sulla piattaforma di e-commerce.

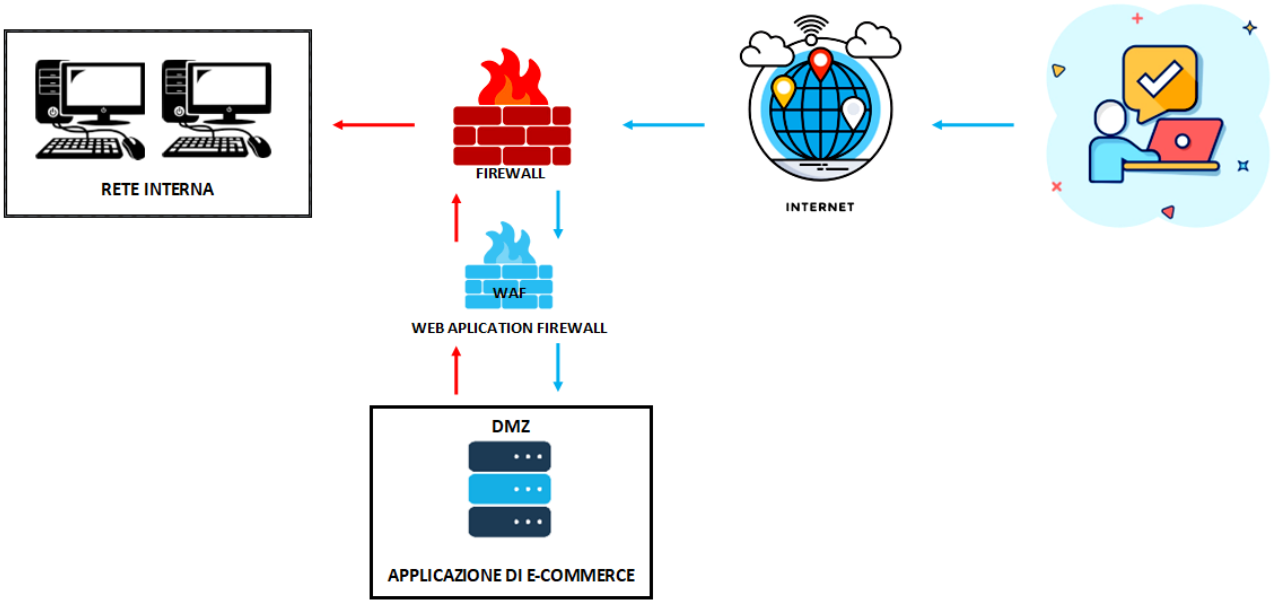
- **Response:**
  La nostra principale preoccupazione è prevenire la diffusione del malware all'interno della rete interna, mentre non intendiamo revocare l'accesso dell'attaccante alla macchina infetta. Modificheremo la figura sulla slide 2 per riflettere questa soluzione proposta.

AZIONI PREVENTIVE

Per prevenire potenziali attacchi alla nostra applicazione Web, un sito di e-commerce ospitato in una DMZ senza protezioni avanzate per facilitare l'accesso degli utenti, proponiamo di introdurre un Web Application Firewall (WAF) lungo il percorso verso la Web application.

I WAF proteggono le applicazioni Web da varie minacce, inclusi attacchi di tipo injection, denial of service (DoS) e traffico dannoso. Questo strumento ci permetterà di definire e gestire regole per mitigare le minacce provenienti da Internet, come indirizzi IP sospetti, testate HTTP, dati inviati tramite HTTP, scripting (XSS), SQL injection e altre vulnerabilità. Il WAF sarà implementato per proteggere l'applicazione Web e raccogliere i log degli accessi per scopi di conformità e analisi.

Le frecce rosse indicano il flusso di comunicazione della rete interna verso la Web application, mentre le frecce azzurre indicano il flusso degli utenti che accedono alla Web application, ovvero al sito di e-commerce.



IMPATTI SUL BUSINESS

L'applicazione Web è soggetta a un attacco di tipo DDoS dall'esterno, causando un'interruzione del servizio per 10 minuti. Per calcolare l'impatto sull'attività dovuto alla non disponibilità del servizio, è stata considerata una spesa media degli utenti sulla piattaforma di e-commerce pari a 1.500 € al minuto.

Impatto = Spesa media x Servizio fuori uso = €1500 x 10 = €15000

Di conseguenza, moltiplicando la spesa potenziale degli utenti per minuto (1.500 €) per i minuti di indisponibilità del servizio (10), si ottiene l'impatto sull'attività complessivo.

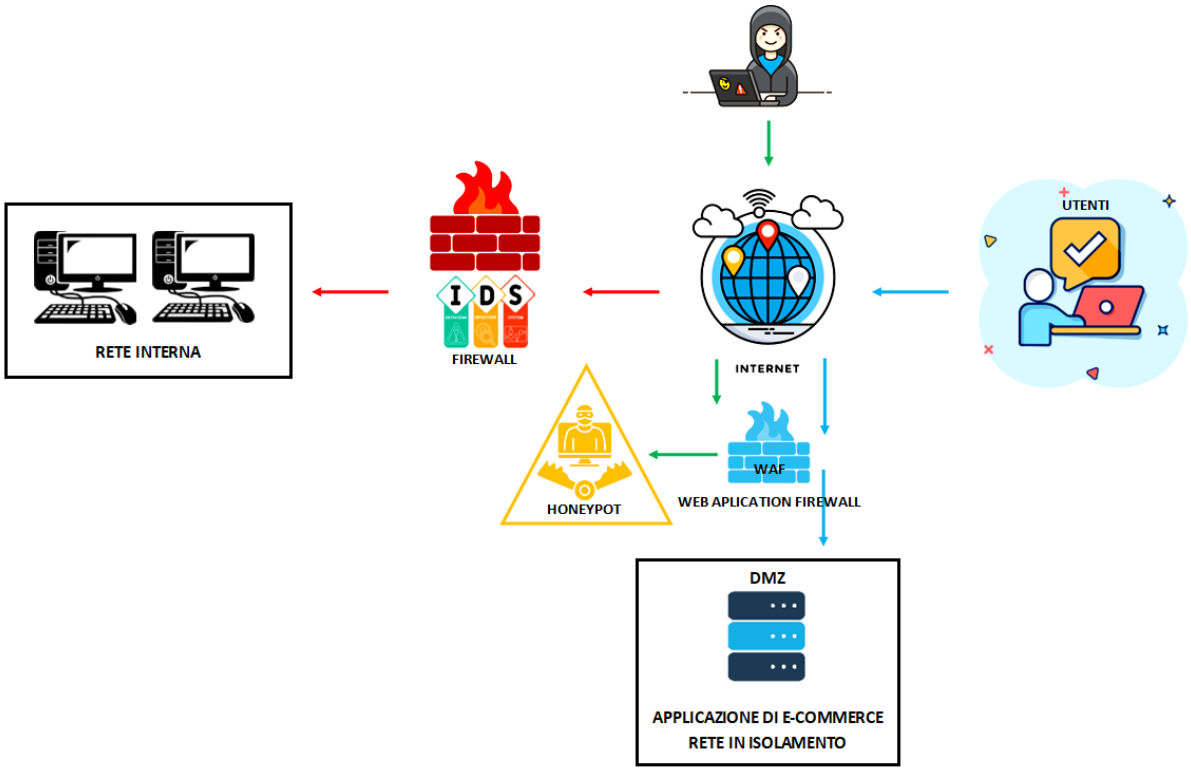
In questo caso, l'impatto sull'attività risulta essere di 15.000 €, indicando che per i 10 minuti di indisponibilità, l'azienda ha subito una perdita di potenziali acquisti pari a 15.000 €.

RESPONSE

Dopo un attacco malware alla nostra applicazione web, è essenziale proteggere la rete interna per prevenire ulteriori danni e proteggere i dati sensibili e i sistemi critici.

Una strategia efficace per farlo è l'isolamento del sistema compromesso. Questo implica separare il sistema infetto dalla rete interna, creando una sorta di "quarantena" che impedisce all'attaccante di accedere ai dati e ai dispositivi critici all'interno della rete. Anche se l'attaccante possa ancora interagire con l'applicazione web compromessa, il suo accesso alla rete interna sarà interrotto, limitando l'impatto dell'attacco e proteggendo la rete interna da ulteriori compromissioni. Inoltre, l'isolamento fornisce il tempo e lo spazio necessari per identificare e risolvere le vulnerabilità nella web app e per ripristinare la sicurezza complessiva del sistema.

Questa soluzione consente all'azienda di limitare i danni tecnici ed economici, consentendo la continuazione del servizio fino a quando non sarà possibile trasferirsi su un nuovo sistema non compromesso o ricostruire la Web application da zero.



Introduciamo un **honeypot** per confondere l'attaccante e indirizzarlo verso una risorsa fittizia, e aggiungiamo sistemi di rilevamento delle intrusioni **(IDS)** insieme al firewall nella rete interna.

Un **Firewall IDS**, o **INTRUSION DETECTION SYSTEM**, è un sistema di sicurezza informatica progettato per monitorare il traffico di rete alla ricerca di pattern anomali o comportamenti sospetti, al fine di identificare e prevenire intrusioni o attacchi informatici.

Un **HONEYPOT** è un'installazione di sistema o rete progettata appositamente per attirare e catturare attacchi informatici, intrusi o altre attività sospette. Funge da esca, simulando vulnerabilità o risorse interessanti per gli attaccanti al fine di monitorare e analizzare le loro tattiche, tecniche e procedure (TTP) senza compromettere effettivamente risorse critiche o dati sensibili.

In sostanza, questa infrastruttura più robusta e controllata protegge la rete e la Web application da ulteriori minacce e fornisce una maggiore visibilità sulle attività sospette per una risposta rapida e mirata.