S9L5

Rosario Zappalà

Indice:

Obiettivi giornalieri:

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

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.

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.

Traccia 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

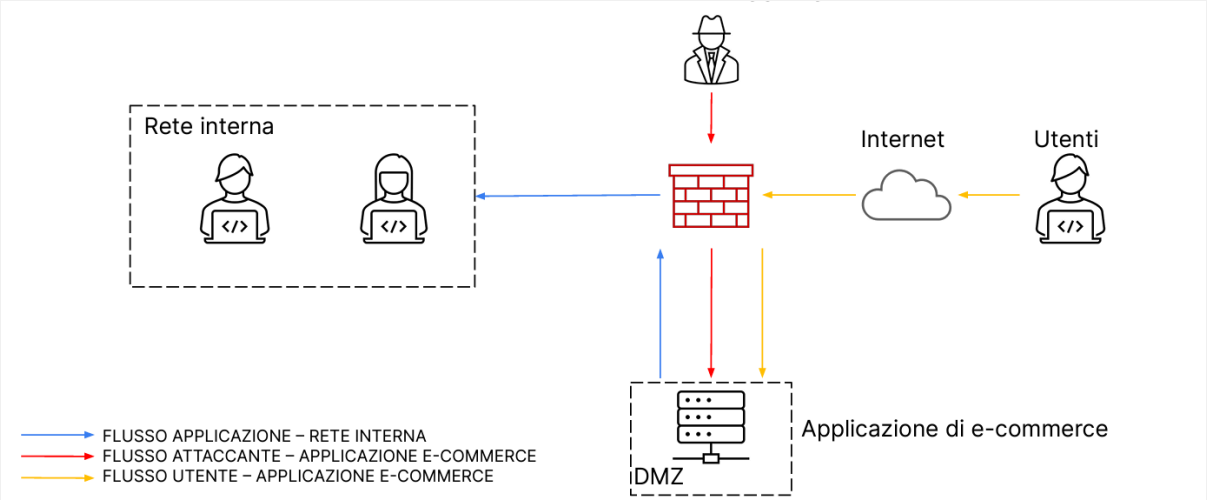


Figura 1

Descrizione Situazione iniziale:

E' possibile notare come la Figura 1 di partenza presenti vulnerabilità che consentono ad utenti malintenzionati di oltrepassare le difese imposte dal Firewall al fine di attaccare la DMZ che contiene il sito E-commerce.

La perdita di un servizio erogato in casi come questo infligge danni economici alle aziende vittima dell'attacco.

Le informazioni fornite non presentano però un quadro molto chiaro della situazione, in quanto:

Nel caso in cui all'interno della DMZ siano presenti ulteriori Web Application, Server MTA o altri dispositivi in generale, sarebbe consigliato suddividere la DMZ in segmenti più piccoli, isolando il sito e-commerce in un proprio segmento.

Questa azione serve a mitigare i rischi legati agli attacchi che vedremo successivamente all'interno del Report.

Dispositivi di sicurezza:

Attenendosi alle informazioni ricevute possiamo considerare le seguenti soluzioni:

- **WAF**

Installare un WAF davanti al sito e-commerce per filtrare il traffico dannoso e bloccare gli attacchi comuni, come ad esempio gli attacchi di tipo SQL injection e cross-site scripting, che sono appunto oggetto della traccia di oggi.

Un WAF (Web Application Firewall) è un sistema di sicurezza progettato per proteggere le applicazioni web da attacchi informatici.

Funziona come un filtro intelligente che analizza il traffico in entrata e in uscita da un applicazione web, bloccando le richieste dannose e consentendo quelle che al contrario sono legittime

Inoltre, il WAF può proteggere da attacchi come SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF) e denial-of-service (DoS).

Tipologie di WAF:

WAF basati su rete:

Vengono installati come appliance hardware o software all'interno della rete e analizzano il traffico di rete a livello di pacchetto.

WAF basati su cloud:

Vengono forniti come servizio in abbonamento da un provider di sicurezza cloud e analizzano il traffico di rete a livello di applicazione.

Nel nostro caso utilizzeremo un WAF basato su rete.

- **(IDS) Sistema di rilevamento delle intrusioni:**

Un IDS (Intrusion Detection System) è un sistema di sicurezza che monitora il traffico di rete e i dispositivi alla ricerca di attività dannose note, attività sospette o violazioni delle politiche di sicurezza.

Funzionamento:

L'IDS analizza il traffico di rete e lo confronta con un database di firme di intrusioni note, ovvero modelli di comportamento che indicano un potenziale attacco. Se l'IDS identifica un'attività sospetta, genera un avviso che può essere inviato a un amministratore di sicurezza o a un sistema di gestione delle informazioni e degli eventi di sicurezza (SIEM).
L'amministratore di sicurezza può quindi esaminare l'avviso e intraprendere le azioni necessarie per rispondere all'incidente.

Vantaggi di un IDS:

Rilevamento tempestivo delle minacce:
l'IDS può identificare le minacce in tempo reale, consentendo di rispondere rapidamente agli incidenti di sicurezza.
Protezione da attacchi sconosciuti:
l'IDS può rilevare attacchi sconosciuti che non sono ancora presenti nel database di firme di intrusioni.

(Si potrebbe pensare persino all'implementazione di un IDPS che svolga anche funzioni da IDS)

- ## (IPS) Sistema di prevenzione delle intrusioni:

Un IPS (Intrusion Prevention System) è un sistema di sicurezza di rete che monitora e analizza il traffico di rete in tempo reale per identificare e prevenire intrusioni e attacchi informatici.

Funzionamento di un IPS:

L'IPS confronta il traffico di rete con un database di firme di intrusioni note, modelli di comportamento che indicano un potenziale attacco.
Se l'IPS identifica un'attività sospetta, può intraprendere diverse azioni per bloccarla, come:

- Bloccare il traffico dannoso all'origine
- Reindirizzare il traffico a un sistema di analisi
- Disattivare temporaneamente i dispositivi vulnerabili
- Inviare avvisi agli amministratori di sicurezza

Monitoraggio e analisi:

Eseguire un monitoraggio costante della DMZ e del sito e-commerce per identificare anomalie o attività sospette potrebbe aiutare a mitigare i rischi corsi e potrebbe aiutare ad intraprendere azioni investigative e penali.
Analizzare i log di sicurezza per identificare eventuali intrusioni o tentativi di accesso non autorizzato può essere decisivo in alcuni casi come metodo per individuare dati.

- ## I File di Log

I log, o file di log, sono registrazioni sequenziali e cronologiche di eventi e attività che avvengono all'interno di un sistema informatico.
Esistono diversi strumenti di analisi dei log che possono facilitare il processo di ricerca e identificazione di informazioni specifiche.
Questi strumenti offrono diverse funzionalità, come ad esempio: Ricerca e filtraggio, Analisi statistica, Visualizzazione,Correzione dei log. per identificare e correggere errori nei log.

Aggiornamenti e patch:

E’ altresì importante assicurarsi che tutti i software e sistemi all'interno della DMZ siano aggiornati con le ultime patch di sicurezza, così facendo potremmo risolvere alcune problematiche legate alla vulnerabilità del codice utilizzato dal software o dal tool utilizzato.

Formazione del personale:

Anche fornire al personale formazione sulla sicurezza informatica può mitigare il rischio di attacchi subiti, sensibilizzando infatti le opinioni sulle azioni da intraprendere in determinati casi specifici, si può aumentare la consapevolezza delle minacce corse .

Configurazione della rete consigliata:

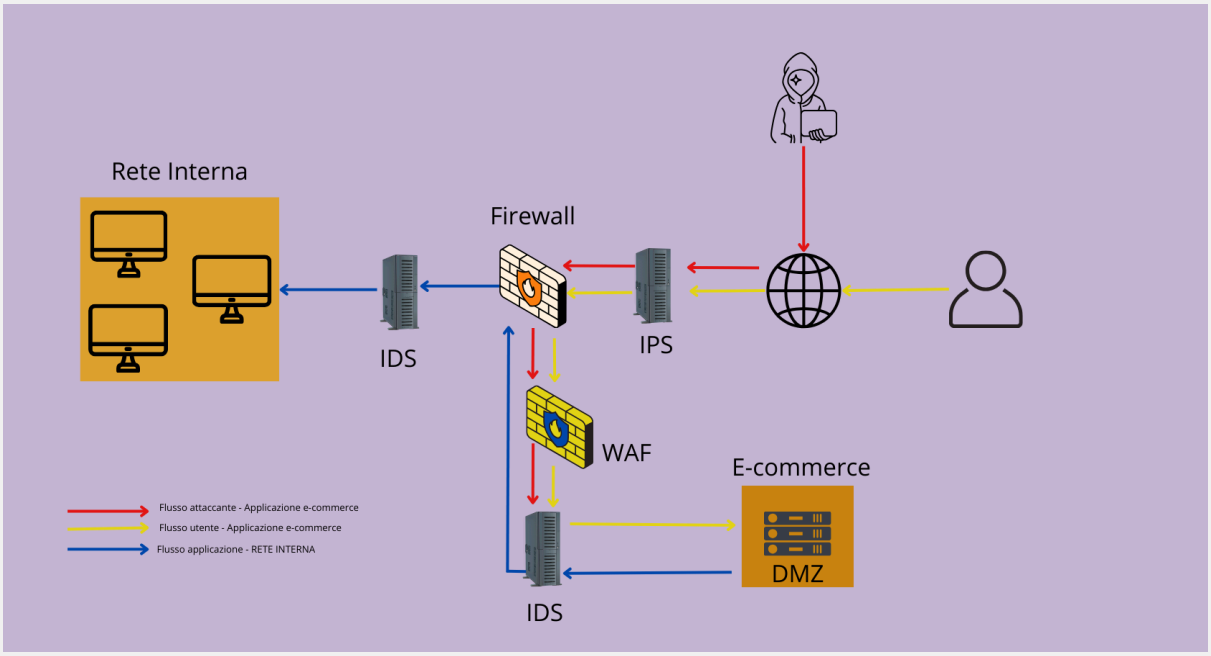


Figura 2

Come da Figura 2, consigliamo l'utilizzo delle seguenti implementazioni, spinti dalle motivazioni e dagli utilizzi già presenti all'interno del Report:

- Implementazione di un IPS subito prima del Firewall già presente.
- Implementazione di un WAF subito dopo il Firewall già presente.
- Implementazione ed uso di un IDS subito dopo il WAF, prima della DMZ.

Approfondimento

La Figura 2 tende a sottolineare il consiglio velato di incrementare i dispositivi di sicurezza anche a protezione della rete interna, in questo caso ci siamo limitati all'implementazione di un IDS a sostegno del già presente IPS e del Firewall. Potrebbe essere interessante posizionare anche la rete interna all'interno di una DMZ.

TRACCIA 2

Calcolare l’impatto sul business:

Considerando che in media ogni minuto gli utenti spendono 1.500 € sulla piattaforma E-commerce e che l’attacco di tipo Ddos causa la non reperibilità della piattaforma per 10 minuti, possiamo stimare così i danni a carico della compagnia:

1.500€ è la spesa potenziale che gli utenti effettuano sul nostro E-commerce di riferimento, ogni minuto.
10 è invece il numero di minuti cui l’attacco dura, nel frattempo il sito sarà dunque irraggiungibile.

Impatto sul business = 1.500 € x 10 minuti = 15.000 €

10 minuti di indisponibilità hanno causato un danno alla compagnia per 15.000 euro (**potenziali**).

Informazioni utili:

Un attacco di tipo Distributed Denial-of-Service (o semplicemente DDoS) è un tentativo di interrompere il normale traffico di un server, servizio o rete, inoltrando quanto più traffico possibile al fine di intasare la connessione, così da rendere il processore del dispositivo sovraccarico e dunque quest’ultimo si ritrova impossibilitato a processare altre richieste da parte questa volta di utenti legittimi.

TRACCIA 3

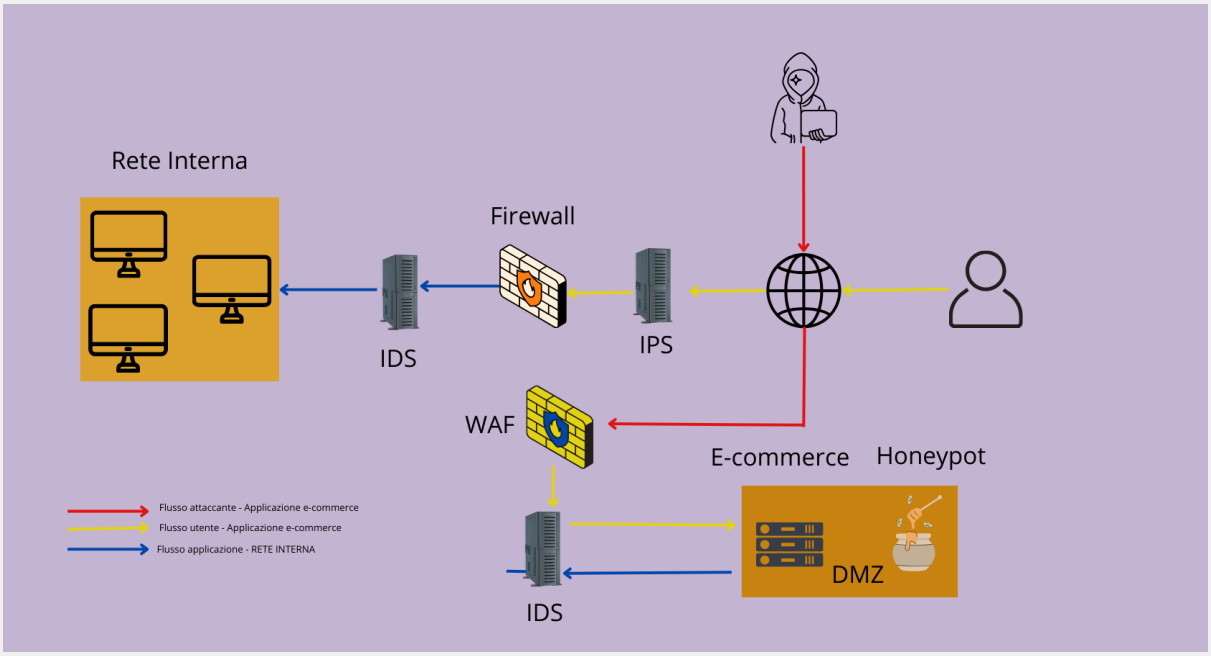
Response:

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 con le evidenze delle implementazioni.

Considerata la priorità, 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.

Nota: In questa situazione agire tempestivamente potrebbe limitare i danni. In questo caso specifico scegliamo di utilizzare l’intrusione del Black Hat Hacker a nostro favore per provare a catturare quante più informazioni possibili sul modus operandi di quest’ultimo ed altre informazioni per quel che invece riguarda la sua macchina in esecuzione.

La trappola!



Creazione di un Honeypot:

- Installare un software "esca" all'interno della DMZ, simulando sistemi e dati sensibili che potrebbero essere di interesse per l’attaccante.
- Settare la configurazione dell’ honeypot per monitorare l'attività dell'attaccante, registrando quante più informazioni possibili sulle sue azioni (dunque anche sulle query che utilizza e sulle directory che visita) ed altre informazioni (nel nostro caso assai più importanti) riguardanti invece le macchine utilizzate dall’attaccante ed altre informazioni utili alle indagini.

Honeypot

Un honeypot, letteralmente "barattolo di miele", è un sistema informatico o una componente hardware o software progettata per attirare hacker malintenzionati, fungendo da esca in un ambiente controllato che mira ad ottenere informazioni sugli attaccanti che possono essere utilizzate in fase offensiva o in fase di indagini penali.

Vanta_Black