CS 0423 - Alex Fiorillo

CONSEGNA S9/L5

Analisi dei log: caso reale

INTRODUZIONE

Con riferimento alla *figura 1*, 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? Modificare la *figura 1* 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. Modificare *figura 1* con la soluzione proposta.

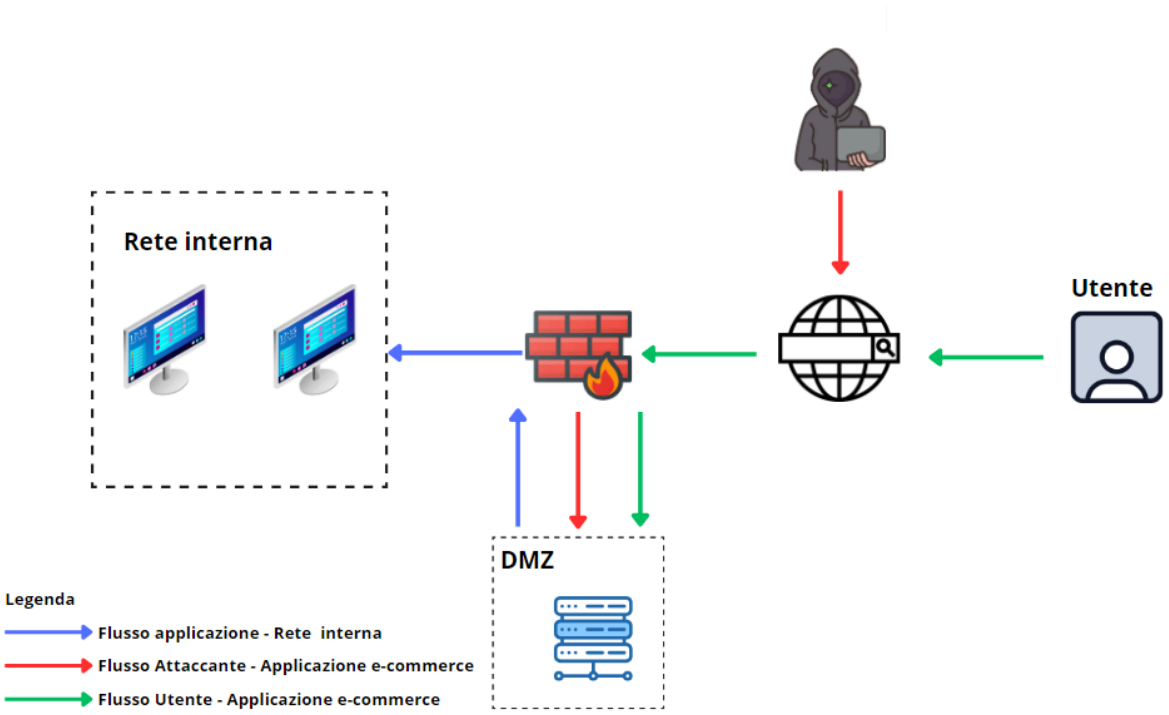

Figura 1

ANALISI SCHEMA DI RETE

Rete interna: parte di un'infrastruttura di rete di un'organizzazione che è protetta da misure di sicurezza informatica per prevenire, rilevare e rispondere alle minacce e agli attacchi informatici provenienti sia dall'interno che dall'esterno dell'organizzazione stessa. Questa rete è considerata il "cuore" dell'ambiente di rete di un'organizzazione e comprende tutti i dispositivi, i server, i database e le risorse interne che sono critici per le operazioni aziendali.

Firewall: componente di sicurezza informatica (hardware, software o entrambi) progettato per monitorare e controllare il traffico di rete tra una rete privata e le altre reti, come Internet o reti aziendali esterne. Il suo obiettivo principale è quello di proteggere la rete interna (o privata) da accessi non autorizzati, intrusioni, malware e altri tipi di minacce informatiche.

Internet.

DMZ: o Demilitarized Zone è una parte di rete che è resa accessibile al pubblico esterno, ma che è separata dalla rete interna dell'organizzazione. Comunemente utilizzata per ospitare servizi e risorse che richiedono accesso dall'esterno.

Attaccante: individuo (o gruppo di individui) che tenta accessi non autorizzati per scopi malevoli.

Utente: utente autenticato e riconosciuto dalla web app per usufruire dei servizi offerti.

CASISTICHE

1. Azioni preventive

Ci viene chiesto di implementare soluzioni per prevenire attacchi di tipo XSS e SQL Injection alla web app.

WEB APP

applicazione software che viene eseguita su un server web e viene accessibile tramite un browser web su Internet o una rete intranet. A differenza delle applicazioni desktop tradizionali, le web app non richiedono di essere installate sui dispositivi degli utenti e possono essere utilizzate da qualsiasi dispositivo connesso a Internet tramite un browser web.

Attacco XSS

o Cross Site Scripting è un tipo di attacco informatico che si verifica quando un attaccante inserisce codice malevolo (solitamente sotto forma di script JavaScript) in pagine web visualizzate da altri utenti. Questo codice malevolo viene eseguito nel browser dell'utente vittima quando visualizza la pagina web compromessa, consentendo all'attaccante di eseguire azioni dannose sul dispositivo dell'utente o di raccogliere informazioni sensibili. Gli attacchi XSS possono assumere diverse forme:

- XSS REFLECTED quando il payload malevolo viene fornito come parte della richiesta HTTP e riflette il codice sul browser dell'utente.
- XSS STORED quando il payload malevolo viene memorizzato sul server web e viene visualizzato a tutti gli utenti che accedono alla pagina compromessa. Ad esempio un attaccante potrebbe inserire un payload XSS in un campo di input su un sito web e il codice malevolo verrebbe eseguito ogni volta che un utente visualizza quella pagina.
- XSS DOM-BASED quando il payload XSS viene eseguito esclusivamente sul lato client, manipolando il DOM (Document Object Model) della pagina web.

Per prevenire attacchi di tipo XSS tutti gli input forniti dagli utenti devono essere attentamente validati prima di essere inclusi in una pagina web che significa che i caratteri speciali e i codici JavaScript all'interno degli input devono essere convertiti in una forma sicura per evitare l'esecuzione non autorizzata di script.
Oltre alla validazione degli input è importante filtrare anche i dati in uscita per assicurarsi che i dati provenienti dal server siano sicuri prima di essere visualizzati nel browser dell'utente.

Attacco SQL Injection

un attacco SQLi è un tipo di attacco che sfrutta le vulnerabilità di sicurezza presenti nelle applicazioni web che interagiscono con database SQL (Structured Query Language). In un attacco SQLi un attaccante inserisce codice SQL malevolo in input destinati a un'applicazione web, sfruttando le lacune nel modo in cui l'applicazione gestisce le query ottenendo così la possibilità di estrarre dati sensibili, modificare o cancellare dati, eseguire comandi sul server o addirittura assumere il controllo dell'applicazione.

Per prevenire attacchi di tipo SQLi si possono adottare pratiche di sicurezza quali la sanitizzazione e la validazione degli input degli utenti, parametrizzazione delle query SQL e l'implementazione di controlli di autorizzazione e autenticazione.

Per proteggere la nostra DMZ/web app possiamo applicare misure preventive basate su **WAF** (Web Application Firewall) a protezione del traffico in entrata da internet sulla DMZ, come possiamo notare in *figura 2*.

WAF

o Web Application Firewall è un tipo di firewall specificatamente progettato per proteggere le web app da una vasta gamma di attacchi informatici, inclusi XSS e SQLi.
Il WAF opera ad un livello più elevato rispetto ai firewall tradizionali poiché analizza il

traffico HTTP e HTTPS destinato alle applicazioni web, identifica e blocca potenziali minacce prima che queste raggiungano l'applicazione stessa.

Schema di rete aggiornato

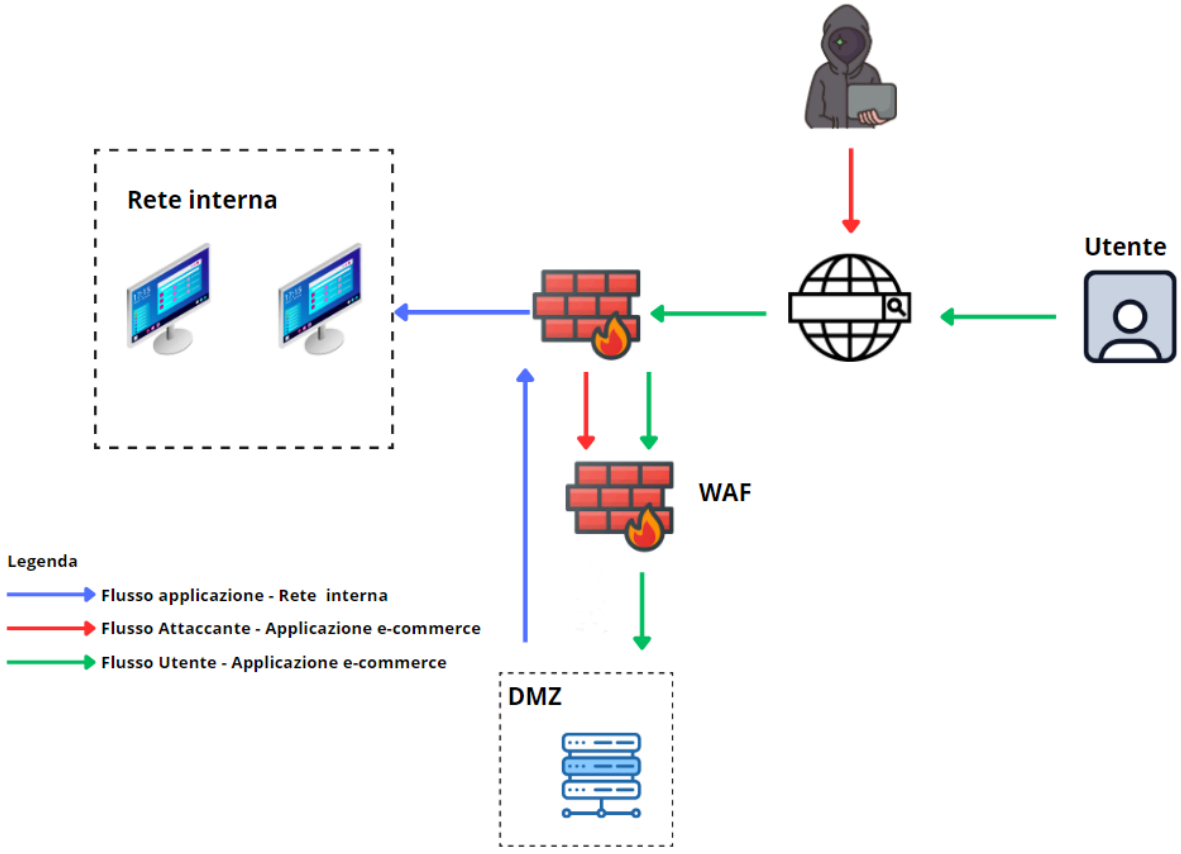

Figura 2

2. Impatti sul business

La nostra applicazione web subisce un attacco **DDoS** dall'esterno che la rende non raggiungibile per 10 minuti.

Attacco DDoS

o Distributed Denial of Service è un tipo di attacco in cui un gran numero di dispositivi, spesso costituiti da botnet o reti di computer compromessi, inviano contemporaneamente una grande quantità di traffico ad un bersaglio specifico come un server web, una rete o un'applicazione online. L'obiettivo di questo attacco è sovraccaricare il target con un'eccessiva quantità di richieste di traffico, rendendolo inaccessibile ai suoi utenti legittimi, a causa di interruzioni del servizio o rallentamento delle prestazioni del sistema.

Per proteggersi dagli attacchi DDoS si possono adottare diverse misure di prevenzione come sistemi di rilevamento degli attacchi, servizi di mitigazione DDoS, configurazione di firewall, filtri di pacchetti per bloccare traffico malevolo e implementazione di sistemi di bilanciamento del carico per distribuire il traffico in modo uniforme così da ridurre l'impatto di un attacco.

Considerando che in media gli utenti spendono **1.500€ al minuto** sulla piattaforma se i servizi rimarranno non raggiungibili per **10 minuti** ci basterà moltiplicare il tempo della durata del disservizio per la media di guadagno al minuto:

Calcolo impatto sul business

tempo disservizio **x** media guadagno al minuto
10 **x** 1.500 **= <u>15.000€</u>**

Per 10 minuti di indisponibilità dei servizi la compagnia ha potenzialmente perso **15.000€** di acquisti.

3. Response

L'applicazione web viene infettata da un **malware.** La nostra priorità è che questo non si propaghi sulla rete, non siamo interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infetta.

Malware

il termine malware nasce dalla combinazione delle parole "**malicious"** (malevolo) e **"software"** e si riferisce a qualsiasi tipo di software progettato per danneggiare, compromettere o alterare il funzionamento di un sistema informatico, di un dispositivo o di una rete, senza il consenso o la conoscenza da parte dell'utente. Un malware può assumere diverse forme e può essere progettato per svolgere una vasta gamma di attività dannose.

I tipi più comuni di malware sono:

- **Virus**
  Si diffonde passando da computer a computer, senza azione diretta o autorizzazione da parte dei sistemi infetti. Si copiano in sezioni particolari all'interno del file system e i più sofisticati cercano di nascondersi dalle analisi dei vari sistemi di sicurezza (come antivirus o anti malware.
- **Trojan**
  Un tipo di malware che si nasconde all'interno di un file apparentemente innocuo, come un documento office oppure un PDS. Si attiva quando la vittima apre il file. Tra i troja più comunemente utilizzati troviamo le backdoor, che sono generalmente utilizzate per fornire agli attaccanti delle shell sui sistemi infetti.
- **Rootkit**
  Un malware progettato per nascondersi dagli utenti e dagli antivirus per prendere il controllo completo del sistema operativo. Un rootkit permette di mantenere privilegi elevati su una macchina senza essere notati.

- **Bootkit**
  Sono dei rootkit che aggirano le protezioni del sistema operativo in quanto entrano in funzione prima dell'avvio completo del sistema operativo, in particolar modo prima dell'attivazione dei moduli di sicurezza di un sistema operativo.
- **Adware**
  Sono dei programmi fastidiosi che mostrano pubblicità agli utenti di un pc.
- **Spyware**
  Programmi che si usano per raccogliere informazioni sulle attività degli utenti di un sistema, ad esempio: il tipo di sistema operativo installato sulla macchina, i siti visitati, le password. Queste informazioni vengono inviate successivamente ad un server sotto il controllo dell'attaccante.
- **Dialer**
  Un programma che cerca di chiamare numeri telefonici a pagamento per guadagnare soldi
- **Keylogger**
  Programma che registra ogni tasto premuto sulla macchina della vittima. I keylogger registrano: i tasti premuti sulla tastiera, il nome delle finestre aperte dall'utente. Salvano poi queste informazioni in un file di log che spediscono ad un server controllato dall'attaccante.

Datosi che la nostra priorità è quella che il malware non si propaghi nella nostra rete pensiamo che la miglior strategia applicabile sia quella di **isolare** la macchina infettata.
La suddetta macchina resterà collegata ad internet e quindi raggiungibile dall'attaccante ma non più connessa alla nostra rete interna, come possiamo notare in *Figura 3*.

Schema di rete aggiornato