S9 L5

Report Progetto

Giulia Salani

INDICE

TRACCIA

Con riferimento alla figura […], rispondere ai seguenti quesiti.

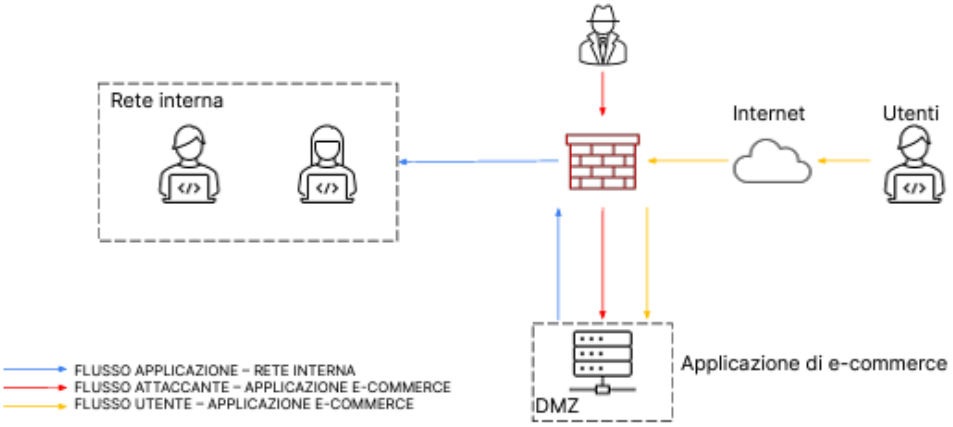
1. Azioni preventive: quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni

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 vostra 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.

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.



REPORT

1. AZIONI PREVENTIVE

1.1 REMINDER CONSEGNA

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.

1.2 DEFINIZIONI: SQLi e XSS

Prima di tutto, **cosa s'intende per attacco SQLi e attacco XSS?**

Un **attacco SQL Injection (SQLi)** è una tecnica di hacking in cui **un attaccante inserisce o manipola del codice SQL malevolo in un'istruzione SQL attraverso input di dati**. L'obiettivo è sfruttare falle di sicurezza nelle applicazioni web che utilizzano input non validati o mal gestiti.

Gli attacchi SQL Injection (SQLi) **possono essere suddivisi in due categorie principali**: Blind SQL Injection e Non-Blind SQL Injection.

1. In un attacco **SQL Injection Blind**, l'attaccante non riceve direttamente i risultati della query nell'output dell'applicazione; sfrutta invece le condizioni booleane nelle query per inferire informazioni sul database.
2. In un **Non-Blind SQL Injection**, l'attaccante riceve direttamente i risultati della query nell'output dell'applicazione, quindi può manipolare direttamente la query per ottenere informazioni, modificare i dati o eseguire azioni dannose.

Nell'**attacco XSS (Cross-Site Scripting)**, invece, **l'attaccante inserisce script malevoli in pagine web visualizzate da altri utenti**. Questi script possono essere eseguiti all'interno del browser degli utenti che visitano la pagina compromessa, consentendo all'attaccante di rubare informazioni sensibili, manipolare il contenuto della pagina, o eseguire azioni dannose a nome dell'utente.

Esistono **tre principali tipi di attacchi XSS**:

Stored XSS (o persistente):

In un attacco di tipo Stored XSS, il payload malevolo è immagazzinato su un server e viene visualizzato ogni volta che un utente accede a una pagina web compromessa.

Reflected XSS (o riflesso):

In un attacco di tipo Reflected XSS, il payload malevolo non è immagazzinato su un server, ma viene riflesso da un'applicazione web e incorporato direttamente nella risposta HTTP.

DOM-based XSS:

Questo tipo di attacco coinvolge la manipolazione del Document Object Model (DOM) lato client. Gli attaccanti sfruttano le vulnerabilità nel codice JavaScript dell'applicazione per eseguire script malevoli nel contesto del DOM.

1.3 AZIONI PREVENTIVE

Le azioni che permettono di prevenire attacchi SQLi e XSS sono molteplici.
Alcune sono specifiche per il tipo di attacco:

➢ Azioni preventive specifiche per SQLi:

Validazione e sanificazione dell'input: Validare e sanificare rigorosamente tutti gli input dell'utente, specialmente quelli utilizzati nelle query SQL.

Parametri del Database e Statement Preparati: Utilizzare parametri del database o statement preparati per eseguire le query SQL.

➢ Azioni preventive specifiche per XSS:

Escape dei dati dinamici: Assicurarsi di eseguire l'escape corretto dei dati dinamici inseriti nelle pagine HTML per prevenire l'esecuzione non intenzionale di script (per "eseguire l'escape" s'intende trasformare caratteri speciali o sequenze di caratteri in una forma che non può essere interpretata come codice eseguibile o come parte di uno script dannoso).

Validazione dell'input e filtraggio: Validare e filtrare attentamente tutto l'input dell'utente, impedendo l'inserimento di script malevoli nella base di dati.

Vi è poi un vero e proprio dispositivo di sicurezza che può aiutare a prevenire tali attacchi:

➢ Web Application Firewall (WAF):

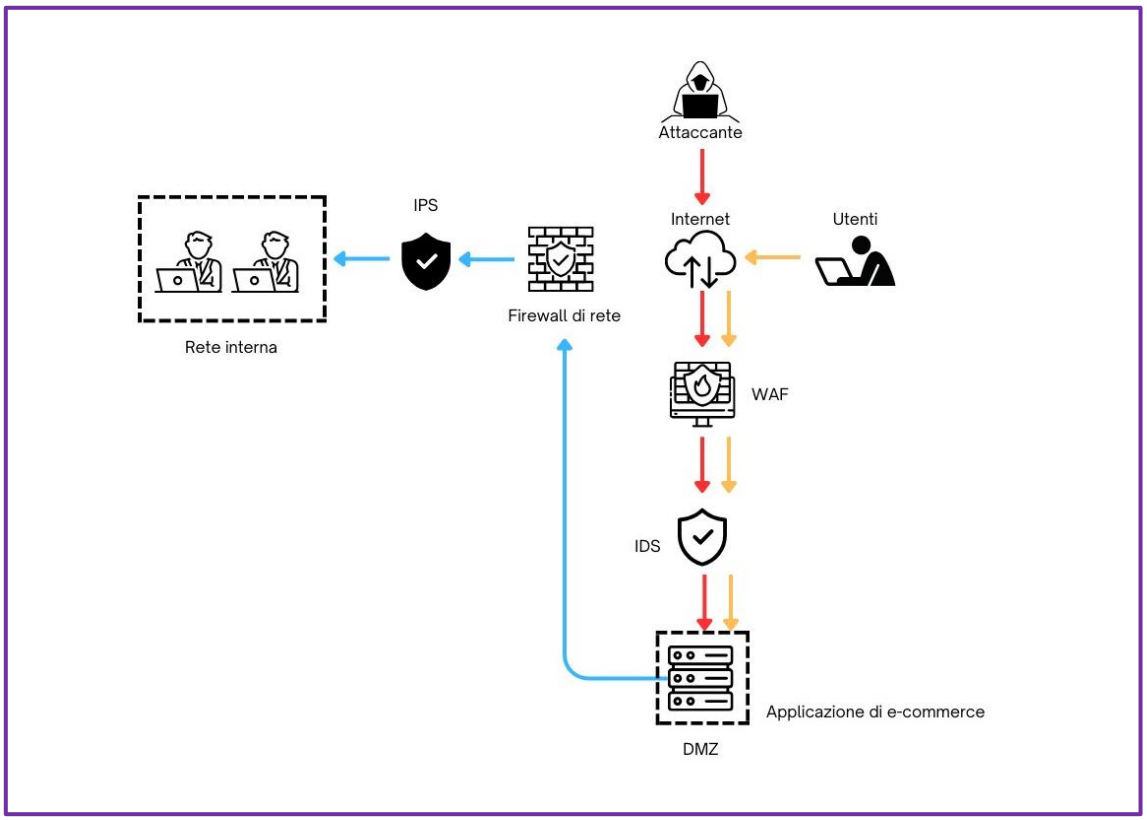
Un **WAF è progettato specificamente per proteggere le applicazioni web**. Si concentra sulla rilevazione e la prevenzione di attacchi diretti alle applicazioni, come SQL Injection, Cross-Site Scripting, e altri attacchi che sfruttano le vulnerabilità delle applicazioni.

Analizza il traffico HTTP/HTTPS a livello applicativo e può applicare regole di sicurezza personalizzate per proteggere da attacchi specifici alle applicazioni.

Nella sezione seguente, vediamo come può essere ridisegnata la rete dell'azienda per assicurare la migliore protezione in termini di sicurezza.

1.4 PROPOSTA DI RETE

Considerato che la consegna non impone limiti di budget, nel riprogettare la rete dell'azienda non è stato solamente inserito un WAF che agisce specificatamente sulle minacce di attacchi SQLi e XSS, ma anche altri due dispositivi di sicurezza, IDS e IPS.



1.5 COMMENTO ALLA PROPOSTA DI RETE

Il design prevede due zone: la rete interna e la DMZ, contenente l'applicazione WEB.
Le zone sono protette ciascuna da due dispositivi di rete, per un totale di quattro dispositivi che commentiamo, inclusa la loro disposizione, di seguito.

1. **IPS tra Firewall di Rete e Rete Interna:**
   L'IPS (Intrusion Prevention System) è un dispositivo o un'applicazione software che monitora il traffico di rete in tempo reale per rilevare e prevenire intrusioni o attacchi informatici. In caso di rilevamento di un comportamento sospetto o di una potenziale minaccia, l'IPS prende misure immediate.
   Posizionato tra il firewall di rete e la rete interna, **l'IPS è in grado di prevenire attivamente il traffico dannoso prima che raggiunga la rete interna**.

2. **Firewall di Rete:**
   Un firewall di rete controlla e filtra il traffico di dati tra una rete interna ed esterna, impedendo accessi non autorizzati e proteggendo dai potenziali attacchi. Utilizza regole predefinite per consentire o bloccare pacchetti in base alle politiche di sicurezza.

Posizionato tra la rete interna e la DMZ per controllare il traffico in ingresso e in uscita, il firewall di rete **protegge la rete interna da possibili minacce provenienti dalla DMZ e da Internet**.

3. **Web Application Firewall (WAF):**
   Come abbiamo visto nella sezione precedente, il WAF è progettato specificamente per proteggere le applicazioni web, analizzando il traffico HTTP/HTTPS. Se ben configurato, è questo il dispositivo che **permette di rilevare e bloccare attacchi specifici alle applicazioni web, come SQL Injection e Cross-Site Scripting.**

4. **IDS tra WAF e DMZ:**
   Un IDS (Intrusion Detection System) è un sistema che monitora il traffico di rete o le attività del sistema alla ricerca di comportamenti sospetti o anomalie che potrebbero indicare una potenziale intrusione o violazione della sicurezza. L'IDS rileva e segnala tali eventi, ma non interviene attivamente per prevenirli.
   Posizionato fra WAF e DMZ, l'IDS **monitora il traffico rilevando potenziali attività sospette o intrusioni nella zona demilitarizzata**. La rilevazione **senza blocco automatico** permette agli amministratori di esaminare le notifiche di allarme e intraprendere azioni correttive, bloccando il traffico solo se lo ritengono necessario.

La configurazione proposta **consente una stratificazione efficace della difesa**, con un focus specifico sulla rilevazione nella DMZ e sulla prevenzione sulla rete interna. La **combinazione di IDS e IPS offre una possibilità di analisi forense approfondita**, consentendo di esaminare attentamente gli eventi rilevati e le azioni preventive intraprese.

Si raccomanda di mantenere sempre aggiornati firewall, WAF, IDS/IPS con le definizioni di attacco più recenti.

2. IMPATTI SUL BUSINESS

2.1 REMINDER CONSEGNA

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.

2.2 DEFINIZIONE: ATTACCO DDOS

Prima di tutto, **cosa s'intende per attacco DDOS?**

DDoS sta per "Distributed Denial of Service" ed è un tipo di attacco informatico in cui **un grande numero di dispositivi o sistemi informatici vengono coordinati per sovraccaricare e rendere inaccessibile un servizio, un sito web o una rete**. Gli attacchi DDoS sfruttano la potenza combinata di molteplici dispositivi per colpire il bersaglio con un elevato volume di richieste, rendendolo incapace di gestire il traffico normale e causando così interruzioni del servizio per gli utenti legittimi.

2.3 IMPATTO SUL BUSINESS

Nel nostro caso, l'applicazione è irraggiungibile per 10 minuti. Se per ogni minuto in media gli utenti spendono 1.500€, moltiplichiamo il valore al minuto per il numero dei minuti e otteniamo l'impatto sul business:

Impatto = 1.500€ x 10 = 15.000€

Quindi, a causa dell'interruzione del servizio per 10 minuti, possiamo stimare che l'azienda abbia perso 15.000€.

2.4 AZIONI PREVENTIVE (EXTRA)

È difficile prevenire completamente un attacco DDoS, ma si possono adottare misure per ridurre il suo impatto o mitigarne gli effetti. Ecco tre misure che vanno in questo senso:

1. **Firewall**: Utilizzare firewall **per bloccare il traffico sospetto** e limitare l'accesso a determinati tipi di pacchetti.
2. **Bilanciatori di Carico e Pianificazione delle Risorse**: L'implementazione di bilanciatori di carico è essenziale per **distribuire equamente il traffico tra più server**, migliorando le prestazioni complessive del sistema. Inoltre, la pianificazione accurata delle risorse, **garantendo riserve adeguate a gestire picchi improvvisi di traffico**, è fondamentale per prevenire la saturazione dei server e mitigare gli effetti di un attacco DDoS. Queste azioni si integrano per ottimizzare la capacità del sistema di gestire il traffico, sia in situazioni normali che durante un attacco.
3. **Rilevamento delle Anomalie**: Implementare sistemi di rilevamento delle anomalie per **identificare rapidamente i modelli di traffico sospetto** e reagire tempestivamente.

3. RESPONSE

3.1 REMINDER CONSEGNA

L'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostra 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.

3.2 DEFINIZIONE: MALWARE

Prima di tutto, **cosa s'intende per malware?**

Il termine "malware" sta per "software dannoso" (malicious software). Si tratta di software progettato con l'intento di danneggiare o compromettere dispositivi, reti o dati, senza il consenso dell'utente. I malware possono assumere varie forme e avere diversi obiettivi, tra cui il furto di informazioni personali, la distruzione di dati, il monitoraggio delle attività dell'utente o il controllo remoto del sistema infetto.

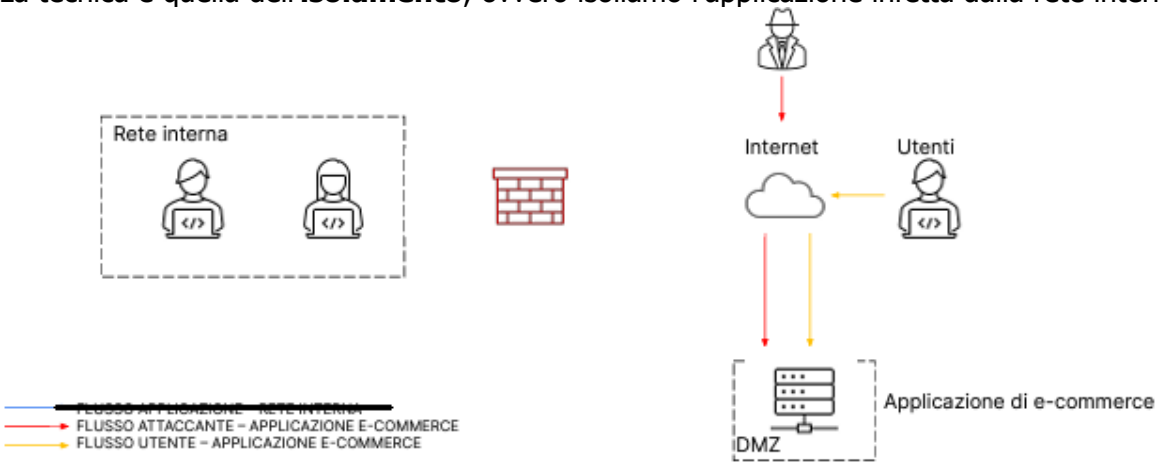
Quando un malware infetta un'applicazione web, può avere diversi effetti dannosi, tra cui:

- **Raccolta di informazioni sensibili** (ad esempio, username e password);
- **Modifiche al funzionamento dell'applicazione** (causando malfunzionamenti, rallentamenti o addirittura blocchi);
- **Distribuzione di altri malware** (ad esempio scaricando e installando altri malware);
- **Utilizzo del sistema infetto per attività dannose** (ad esempio, utilizzandolo per una botnet in un attacco DDoS);
- **Ransomware** (ovvero potrebbe crittografare i file dell'utente e richiedere un riscatto)

3.3 ISOLAMENTO

In questo caso, siamo oltre le azioni preventive perché il sistema è già stato infettato. Ci è stato richiesto di impedire che il malware si propaghi sulla nostra rete, ovvero sulla rete interna.

La rete interna è raggiungibile dalla DMZ per le policy sul firewall. Per impedire al malware di propagarsi sulla rete interna, **dobbiamo interrompere la comunicazione fra DMZ e rete interna**.
La tecnica è quella dell'**isolamento**, ovvero isoliamo l'applicazione infetta dalla rete interna:



3.4 AZIONI DI RIPRISTINO (EXTRA)

Ora che la web app è isolata dalla rete interna per prevenire la diffusione del malware su altre parti del sistema, è necessario intervenire per tornare alla normalità.

Si consigliano le seguenti azioni correttive:

Identificazione: Identificare la natura del malware, compreso il tipo e gli obiettivi specifici, per comprendere appieno l'entità dell'infezione.

Backup e Ripristino: Ripristinare l'applicazione e i dati da un backup pulito precedente all'infezione per eliminare il malware.

Analisi del Codice: Esaminare il codice sorgente dell'applicazione per individuare eventuali modifiche apportate dal malware. Correggere il codice danneggiato o compromesso e verificare la sicurezza dell'applicazione attraverso un'analisi approfondita.

Scanner Antimalware: Utilizzare scanner antimalware aggiornati per eseguire una scansione completa del sistema e assicurarsi che tutti i componenti siano privi di malware (inclusa la rete interna).

Password e Credenziali: Cambiare tutte le password e le credenziali associate all'applicazione, inclusi account utente, password del database e credenziali di accesso a server. Naturalmente le nuove password dovranno soddisfare i criteri di robustezza.

Monitoraggio Continuo: Mantenere sistemi di monitoraggio continuo per rilevare eventuali attività sospette.

L'azienda dovrebbe in ogni caso avere, e se non ce l'ha crearlo, un **Piano di Risposta agli Incidenti** dettagliato con le policy (a livello strategico) e le procedure (a livello tattico/operativo) da attivare in caso di incidente.

IMPATTI SUL BUSINESS

Il progetto settimanale si è sviluppato su 3 fasi.

Nella prima, abbiamo analizzato le azioni preventive da implementare per prevenire attacchi SQLi e XSS alla web app dell'azienda. Dopo aver ripreso le definizioni di questi attacchi, la rete dell'azienda è stata riprogettata inserendo non solo un WAF, ma anche altri dispositivi di sicurezza (IPS e IDS) per irrobustirla al meglio.

La seconda task ha previsto invece il calcolo dell'impatto economico di un'interruzione del servizio di e-commerce causata da un attacco DDoS. Per soli 10 minuti di interruzione, il danno stimato è di 15.000€.

Infine, è stato necessario isolare l'applicazione web dalla rete interna dopo un attacco malware. Anche se non esplicitamente richiesto, oltre a mostrate la tecnica di isolamento, abbiamo anche esplorato le azioni di ripristino per riportare il sistema alla normale operatività dopo l'incidente di sicurezza.