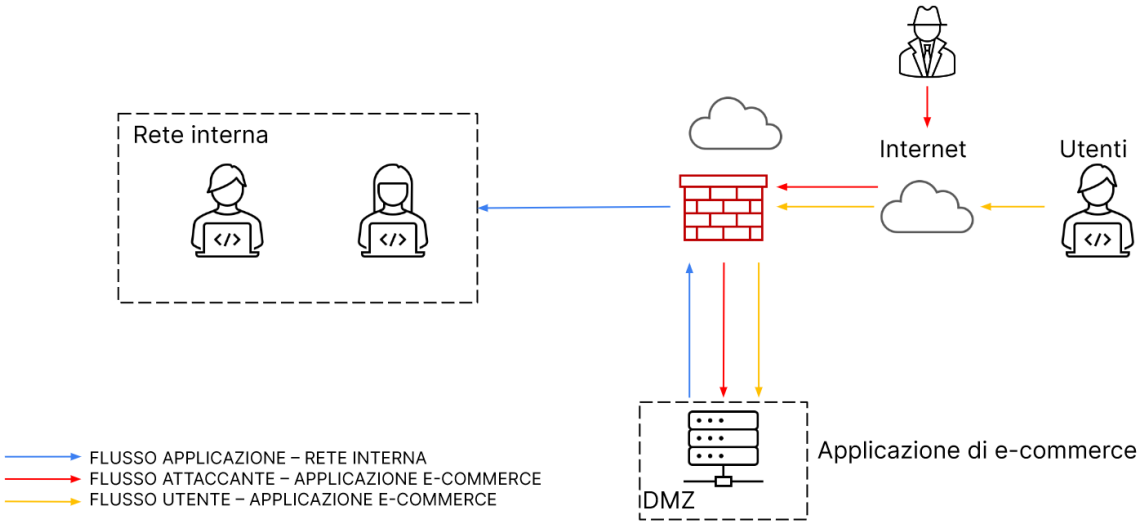
Analisi architettura di rete e misure di sicurezza

Sommario

Introduzione



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.

Problema 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

Considerazioni Generali

Nello schema sopra vediamo che la struttura della rete aziendale comprende una rete segmentata. Esiste una DMZ (Demilitarized Zone / Zona Demilitarizzata) nella quale risiede il server dell'applicazione di e-commerce.

La DMZ funge da buffer tra la rete interna e la rete esterna, offrendo un ulteriore livello di sicurezza. Le risorse che sono accessibili al pubblico generale, come in questo caso l'applicazione di e-commerce, vengono solitamente posizionate nella DMZ, mentre le risorse interne critiche, come i database e i sistemi di backend, rimangono protette all'interno della rete interna. In pratica, se un attaccante riuscisse a compromettere un sistema all'interno della DMZ, non avrebbe automaticamente accesso alla rete interna, poiché ci sono ulteriori misure di sicurezza e firewall tra la DMZ e la rete interna.

In questo caso, le policy impostate sul firewall rendono raggiungibile la rete interna dalla DMZ, dando modo ad un potenziale attaccante di raggiungere a rete interma nal caso in cui riuscisse a compromettere il server dell'applicazione e-commerce.

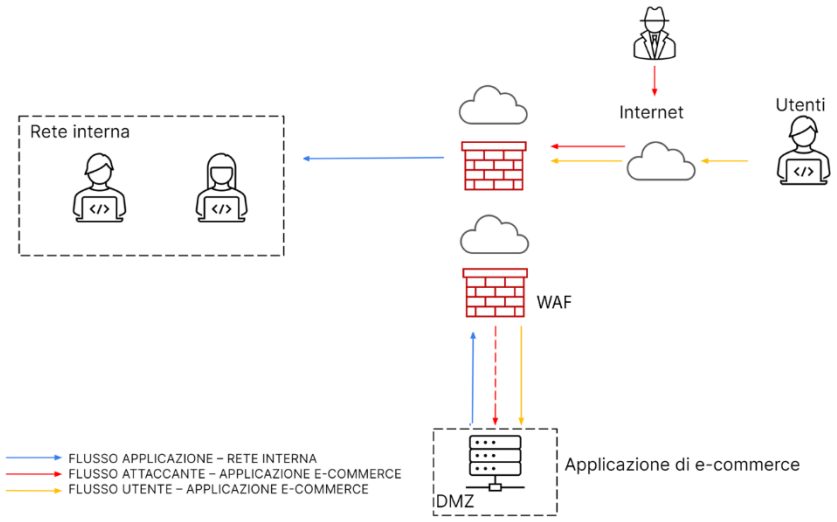
Dal momento che l'applicazione di e-commerce deve essere disponibile per gli utenti tramite Internet per effettuare acquisti sulla piattaforma, l'accesso a Internet dalla DMZ deve ovviamente rimanere aperto. Con questa configurazione e senza altre misure preventive, non risuciamo a distinguere un utente che accede regolarmente da Internet per fare acquisti sulla piattaforma da un eventuale malintenzionato che accede per effettuare un attacco di tipo SQLi oppure XSS. Di seguito si riportano alcune misure preventive mirate alla riduzione della probabilità che avvenga questo tipo di attacchi.

Misure di sicurezza preventive

Di seguito si riportano le principali misure di sicurezza preventive per la riduzione del rischio di un attacco di tipo SQLi o XSS all'applicazione e-commerce.

Utilizzo di Web Application Firewall (WAF)

Per difendere l'applicazione web da potenziali attacchi di questo tipo, una misura che potrebbe essere preventivamente adottata è l'utilizzo di un Web Application Firewall (WAF), in aggiunta al firewall già esistente, come mostrato nello schema sotto.



Un Web Application Firewall (WAF) è una soluzione di sicurezza specificamente progettata per proteggere le applicazioni web da una vasta gamma di attacchi, tra cui SQLi e XSS.

Mentre i firewall tradizionali si concentrano principalmente sul traffico a livello di rete, i WAF si focalizzano sul traffico a livello di applicazione. Un WAF analizza il traffico HTTP/HTTPS diretto all'applicazione web, cercando schemi o comportamenti sospetti e viene generalmente posizionato tra l'applicazione web di un utente e il traffico web che la raggiunge.

Può essere implementato come un dispositivo hardware, un servizio cloud o come software sullo stesso server dell'applicazione.

Code analysis (analisi del codice sorgente) / Penetration testing e patching del sistema

La sanificazione degli input, ovvero la pulizia e validazione degli input utente, è fondamentale per prevenire vulnerabilità come SQL Injection (SQLi) e Cross-Site Scripting (XSS).

Attraverso l'analisi del codice della web application è possibile identificare i punti di ingresso, ovvero tutti i punti in cui l'applicazione accetta input dall'utente, e verificare se l'input viene correttamente sanificato prima di essere utilizzato in operazioni sensibili, come l'elaborazione di query SQL o la visualizzazione di contenuti sulle pagine web.

In alternativa, è possibile effettuare un penetration testing mirato sulla web application, al fine di rilevare input utente non sanificati e quindi vulnerabilità ad attacchi SQLi e XSS.

A seguito delle suddette verifiche, nel caso le vulnerabilità siano confermate è possibile procedere al patching del sistema. In questo scenario, il patching consiste nell'apportare modifiche al codice della web application per sanificare l'input utente e ridurre il rischio di attacchi SQLi e XSS.

Problema 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. Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica

BIA Business Impact Analysis

Considerando che la piattaforma genera un intorito di 1.500€/min e che l'attacco DDos interrompe i servizi per 10 minuti, l'impatto economico dovuto alla non raggungibilità del servizio ammonta a

1.500 € x 10 = 15.000 €

In dettaglio, utilizzando i parametri standard dell'analisi quantitiva della BIA (Business Impact Analysis), si ha:

- **AV Asset Value** : Valore dell'asset

  Considerando che la piattaforma genera un intorito di 1.500€/min, ragionando su base giornaliera (24h/1.440 min) si ha un introito di

  1.500 € x 1.440 min = 2.160.000 €

- **EF Exposure Factor**: Percentuale di asset che verrebbe impattato a seguito del verificarsi di un determinato evento

  Considerando che in questo scenario l'attacco DDos rende la piattaforma non raggiungibile per 10 minuti, ragionando su base giornaliera (24h/1.440 min) la percentuale di esposizione è data da

  10 min / 1.440 min= 0,6944444 %

- **Single Loss Expectancy (SLE):** Perdita che si subirebbe al verificarsi dell'evento, prodotto tra il valore dell'asset (AV) e la percentuale impattata in caso di evento (EF)

  Abbiamo calcolato AV ed EF, calcoliamo ora SLE con la seguente formula:

  SLE = AV * EF = 2.160.000 € x 0,6944444 % = 15.000 €

  L'attacco DDos genera una perdita attesa di 15.000 € (ovvero 1.500 € /min x 10 min)

- **Annualized Rate of Occurrence (ARO):** Numero di volte stimato dell'evento in un anno.

  In questo scenario ipotizziamo 1 solo attacco di questa tipologia e con queste caratteristiche.

- **Annualized Loss Expectancy (ALE):** Valore della perdita subita in un arco temporale di un anno.

  Considerando che si ipotizza uno scenario con un solo evento di questo tipo, abbiamo:

  ALE = SLE x ARO = 15.000 € x 1 = 15.000 €

  Dunque in questo caso ALE = SLE, ovvero la perdita che si subirebbe al verificarsi di questo attacco corrisponde alla perdita annualizzata.

Misure di sicurezza preventive

Un attacco DDos (Distributed Dos) consiste nella trasmissione contemporanea di un numero ingente di pacchetti alla machina target da sorgenti multiple allo scopo di saturare la CPU portandola al 100% impedendole così di processare altre richieste.

Al fine di ridurre le possibilità che un attacco DDos si verifichi, è possibile adottare una serie di misure di sicurezza preventive specifiche per questo tipo di attacco. Di seguito si elencano le principali. E' consigliabile utilizzare una di queste misure in combinazione ad una o più delle altre per una maggiore sicurezza.

Monitoraggio della rete

Ai fini della sicurezza è, in generale, importante monitorare costantemente lo stato della rete. Nel caso specifico, esistono indicatori di compromissione che indicano un probabile attacco DDoS in corso, come ad esempio un numero molto elevato di richieste TCP, UDP provenienti contemporaneamente da diversi indirizzi ip.
Il monitoraggio della rete è quindi essenziale per rilevare immediatamente questi tipi di attacco ed essere in grado di intervenire tempestivamente. Possiamo utilizzare strumenti come NetFlow, RMON e SNMP per catturare il traffico di rete gestito dai router (router-based monitoring), o esguire attivamente richieste sulla rete (active monitoring) tramite tools come ping o iPerf, oppure utilizzare utilities di monitoraggio di rete (network monitoring tools) come Wireshark.

Firewall a stato

E' possibile utilizzare firewall di rete per bloccare traffico non desiderato. I firewall avanzati, come firewall a stato (o stateful) possono rilevare e bloccare volumi di traffico sospetti o schemi di traffico associati agli attacchi DDoS. I firewall a stato, oltre al controllo dei pacchetti in base alle regole impostate su indirizzi ip e porte, includono altre informazioni sulla connessione. Un esempio sono i Next Generation Firewall (NGFW), che possono acquisire informazioni provenienti da altri sistemi, oltre a ispezionare più caratteristiche di traffico per applicare le policy firewall a livelli più elevati rispetto a un firewall tradizionale. Le informazioni aggiuntive e un livello più approfondito di ispezione di questi firewall consentono di identificare e prevenire anche gli attacchi DDos.

Web Application Firewall (WAF)

Mentre un firewall di rete si concentra su traffico a livello di rete, un WAF monitora e blocca qualsiasi traffico HTTP dannoso in entrata, impedendo al contempo l'uscita di dati non autorizzati dall'applicazione. Di conseguenza, i WAF proteggono le applicazioni business-critical e i server web da varie minacce, tra le quali gli attacchi DDoS.

Sistemi di Rilevazione e Prevenzione delle Intrusioni PS / IDS

Un IDS (Intrusion Detection System) e un IPS (Intrusion Prevention System) sono dispositivi o applicazioni che monitorano il traffico di rete alla ricerca di attività sospette e potenzialmente dannose.

Quando si tratta di attacchi DDoS, un IDS e un IPS possono rilevare - e in alcuni casi mitigare - tali attacchi. Un IDS permette di rilevare schemi di traffico insoliti che potrebbero indicare un attacco DDoS in corso. Questo potrebbe includere un aumento repentino del traffico, traffico da molteplici fonti, o pattern di traffico specifici. Analogamente, un IPS può rilevare l'attacco, ma ha anche la capacità di bloccare attivamente il traffico dannoso.

Problema 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 in slide 2 con la soluzione proposta.

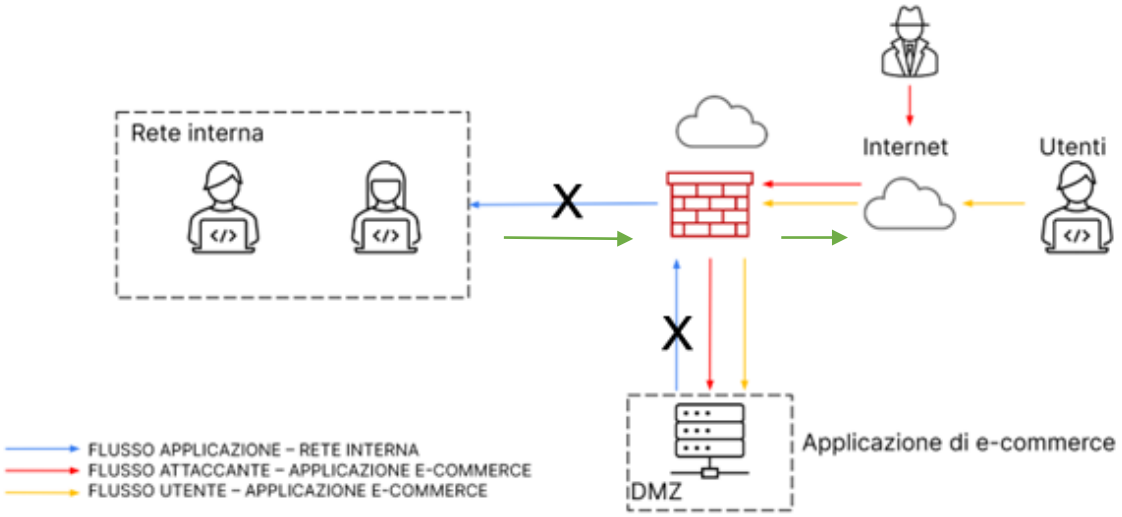
Soluzione proposta

Si propone inizialmente di applicare una strategia di contenimento dell'incidente. La rete è già segmentata e l'applicazione infetta si trova già in un'area di rete ad hoc, la DMZ. Possiamo quindi bloccare immediatamente tutto il traffico dalla DMZ alla rete interna e viceversa tramite l'impostazione di regole specifiche sul firewall.

Questo impedisce al malware di propagarsi alla rete interna, pur lasciando l'accesso da parte dell'attaccante alla web application.

Questa è la soluzione con impatto aziendale minimo per contenere l'incidente e permettere, nel contempo, lo studio del malware e quindi procedere con le fasi di rimozione e ripristino.

Con questa soluzione la rete interna resta connessa a internet passando dal firewall (come mostrano le frecce verdi nell'immagine), pur subendo il disservizio di non avere più accesso al server dell'applicazione e-commerce.



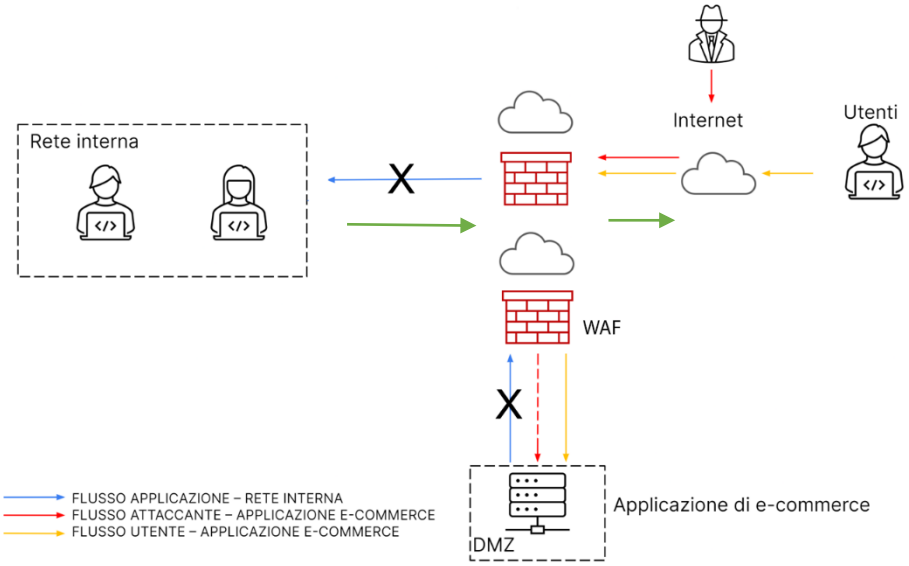
Qualora dovesse risultare necessario, altre soluzioni più stringenti ma con maggiore impatto aziendale sono:

- disconnettere completamente l'applicazione infetta dalla rete aziendale lasciando l'applicazione connessa a internet (tecnica di isolamento), in modo da restringere ulteriormente le possibilità di accesso alla rete interna da parte dell'attaccante;

- se le misure precedenti non risultassero sufficienti, rimuovere il sistema sia dalla rete interna che da internet, rendendolo completamenta irraggiungibile.

Problema 4.

***Soluzione completa**: unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)*

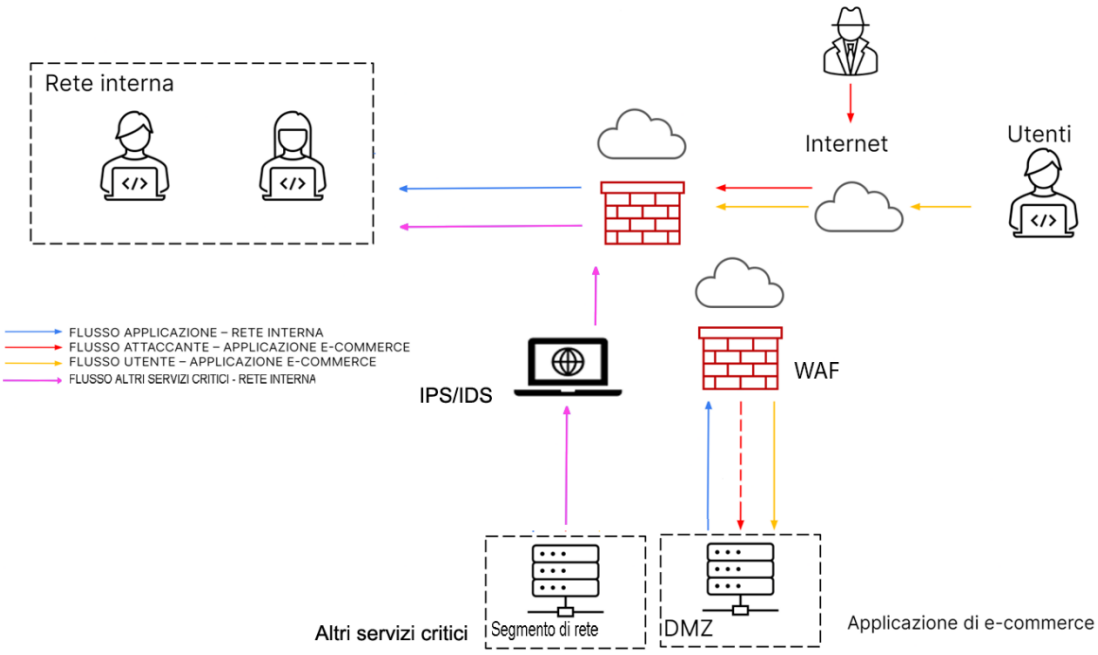


La soluzione nell'immagine riproduce lo scenario in cui il server DMZ è infettato da malware ed è stato isolato dalla rete interna pur restando accessibile dagli utenti web, compresi eventuali attaccanti. Questo impedisce al malware di diffondersi nella rete interna, facendo in modo che resti confinato nella rete DMZ in modo che possa essere studiato e poi che si possa procedere con le fasi di rimozione e ripristino.

La presenza di un Web Application Firewall, nel contempo, protegge il server della web application da eventuali attacchi SQLi e XSS. In questo caso, questi attacchi non andrebbero ad impattare la rete interna. La presenza del WAF però fa in modo che il server della web application infetto da malware non venga compromesso da ulteriori attacchi che possano compromettere lo studio del malware o rallentare, se non addirttura impedire, le fasi di rimozione e ripristino, rendendo necessari interventi di sicurezza più pesanti.

Problema 5.

Modifica «più aggressiva» dell'infrastruttura (se necessario/facoltativo magari integrando la soluzione al punto 2)



Questa soluzione prevede lo spostamento degli altri servizi critici aziendali in un segmento di rete seprarato protetto da un dispositivo IPS o IDS.

Le policy del firewall permettono la comunicazione con la rete interna sia al server e-commerce che al segmento di rete, ma non permettono la comunicazione tra segmento di rete e server e-commerce se non strettamente necessario. Per questo tipo di comunicazione dovrebbe essere adottata la politica del minimo privilegio, ovvero dovrebbero essere consentite soltanto le minime comunicazioni strettamente necessarie all'operatività aziendale.

La separazione dei servizi critici dalla rete interna permette di applicare controlli di sicurezza specifici e più stringenti a quel segmento, come un sistema di rilevazione o prevenzione delle intrusioni (IPS/IDS).

Se, nonostante le misure di sicurezza adottate, un attaccante tramite l'applicazione e-commerce riuscisse a penetrare nella rete interna, l'isolamento dei servizi critici in un altro segmento riduce notevolmente il rischio che riesca a raggiungere o compromettere quei servizi.

Inoltre, con i servizi critici in un segmento separato risulta più semplice monitorare il traffico e le attività legate a quei servizi, permettendo una rilevazione più rapida di comportamenti sospetti o anomalie.