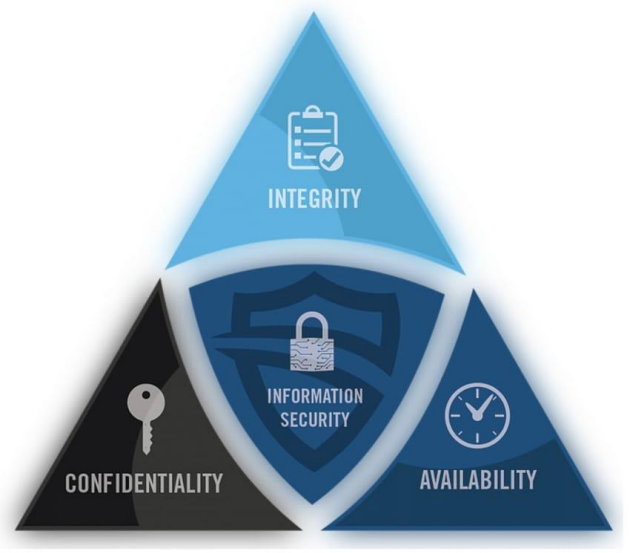
Prevenzione, Analisi e Rimedi



INDICE

ESERCIZIO

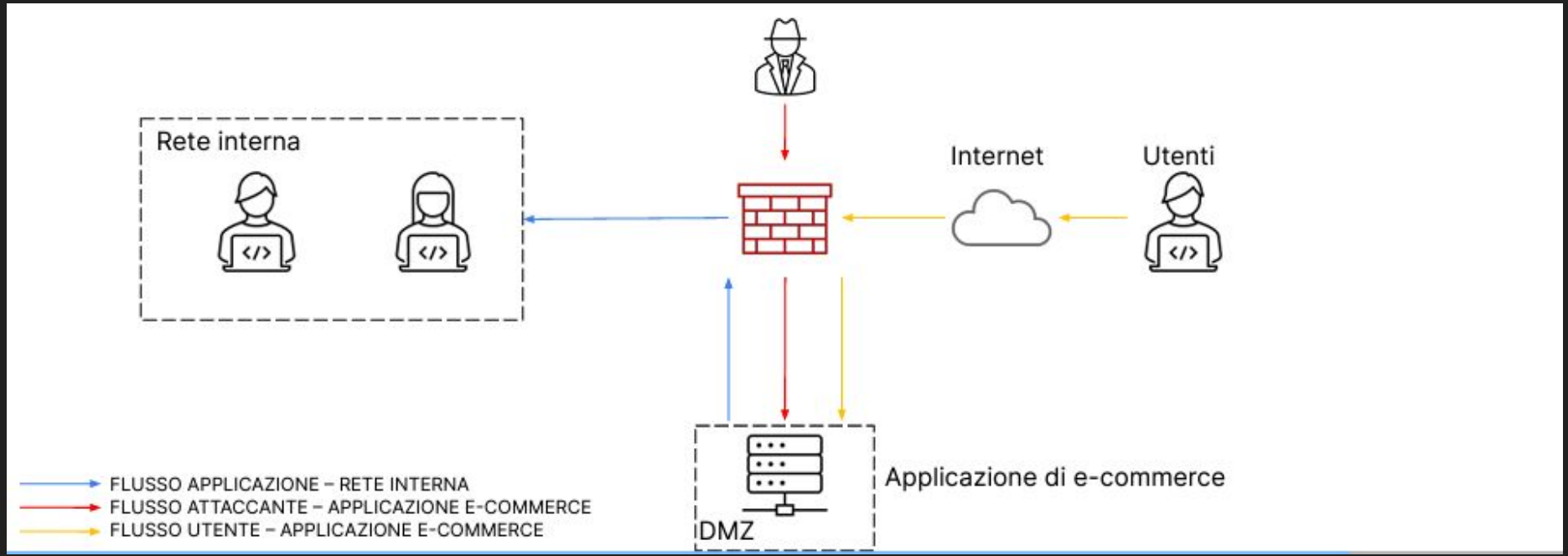
Con riferimento alla figura in slide 4, rispondere ai seguenti quesiti.

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 vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura in slide 4 con la soluzione proposta.

ARCHITETTURA RETE



AZIONI PREVENTIVE

Prima di passare allo svolgimento del primo punto dell'esercizio è bene chiarire cosa siano attacchi di tipo XSS e SQLi

Cross-Site Scripting (XSS):

Contesto: Si verifica quando un'applicazione web incorpora input non validato da un utente all'interno di una pagina web e il browser dell'utente esegue lo script incorporato.
Obiettivo: L'obiettivo principale è eseguire script lato client nell'ambiente del browser dell'utente, spesso per rubare informazioni, cookie di sessione o eseguire azioni dannose a nome dell'utente.
Esempio: Se un'applicazione mostra un commento senza sanitizzare l'input, un attaccante potrebbe inserire uno script JavaScript malevolo che viene poi eseguito quando un altro utente visualizza il commento compromesso.

Iniezione SQL:

Contesto: Si verifica quando un'applicazione web incorpora input non validato da un utente all'interno di una query SQL che viene eseguita su un database.
Obiettivo: L'obiettivo principale è eseguire comandi SQL non autorizzati sul database, spesso per ottenere, modificare o eliminare dati.
Esempio: Se un'applicazione utilizza input utente per costruire una query SQL senza sanitizzare l'input, un attaccante potrebbe inserire una stringa che altera la query originale e ottiene accesso non autorizzato a dati nel database.

AZIONI PREVENTIVE

Differenze principali tra XSS e SQLi:

Ambito dell'Attacco: XSS si concentra sull'esecuzione di script lato client nei browser degli utenti, mentre Iniezione SQL si concentra sull'esecuzione di comandi SQL non autorizzati sul database.
Rischi Associati: XSS può compromettere la sicurezza dell'utente e rubare informazioni sensibili, mentre Iniezione SQL può compromettere l'integrità e la riservatezza dei dati nel database.

In generale, entrambe le vulnerabilità richiedono un'adeguata gestione e validazione degli input per impedire agli attaccanti di inserire dati malevoli.

AZIONI PREVENTIVE

Quali azioni preventive si potrebbero implementare per difendere l’applicazione Web da attacchi di tipo XSS?

Contro Cross-Site Scripting (XSS):

Validazione degli Input: Validare e filtrare rigorosamente tutti gli input utente per prevenire l'inserimento di script dannosi.

Escape Output: Utilizzare funzioni di escape HTML appropriate quando si visualizzano dati dinamici nella pagina web. Ad esempio, `htmlspecialchars` in PHP.

Educare gli Sviluppatori: Fornire formazione continua agli sviluppatori sulle migliori pratiche di sicurezza per evitare errori di programmazione che potrebbero portare a vulnerabilità XSS.

Firewall delle Applicazioni Web (WAF): Utilizzare un WAF per filtrare e bloccare attacchi XSS. I WAF possono rilevare pattern di attacco comuni e proteggere l'applicazione.

AZIONI PREVENTIVE

Quali azioni preventive si potrebbero implementare per difendere l’applicazione Web da attacchi di tipo SQLi?

Contro SQL Injection (SQLi):

Utilizzo di Parametrizzazioni nelle Query SQL: Utilizzare query parametrizzate o prepared statements per garantire che i parametri utente vengano trattati come dati e non come istruzioni SQL.

Validazione e Filtro degli Input Utente: Implementare controlli di validazione e filtraggio sugli input utente per rilevare e bloccare caratteri o strutture sospette.

Firewall delle Applicazioni Web (WAF): Utilizzare un WAF per filtrare e bloccare attacchi SQLi. I WAF possono rilevare pattern di attacco comuni e proteggere l'applicazione.

AZIONI PREVENTIVE

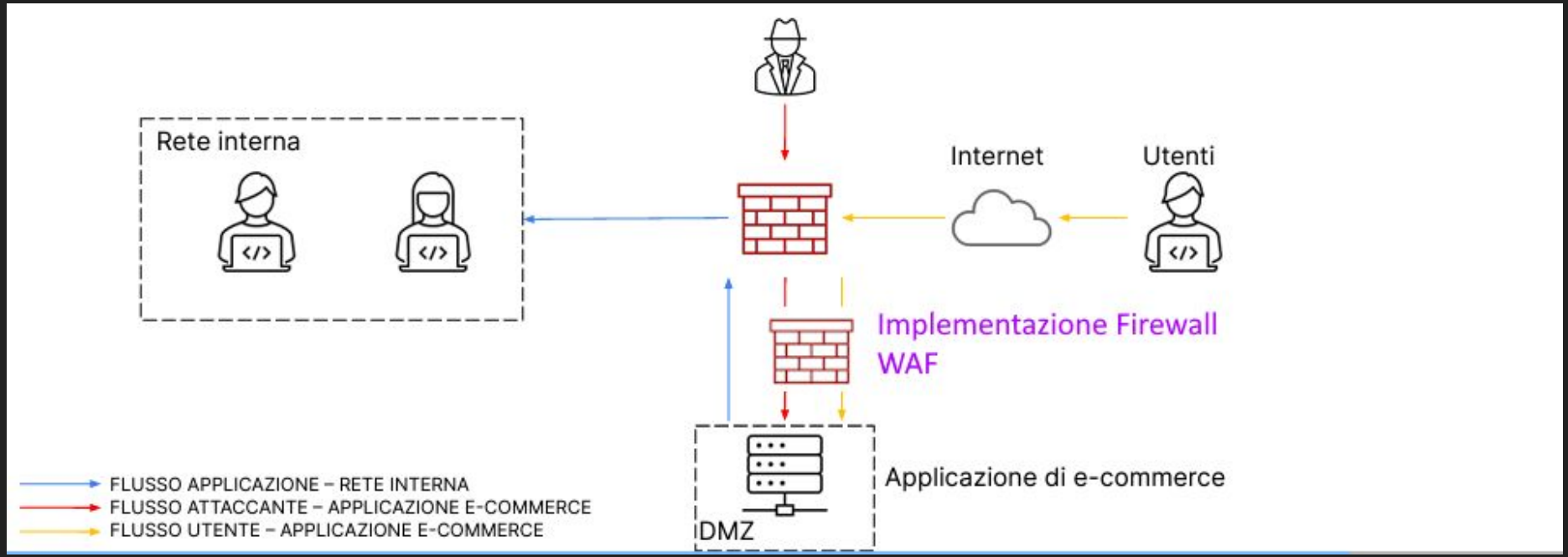
Ora modifichiamo l’architettura di rete in modo da implementare un Firewall per la protezione della Web App da minacce quali XSS e SQLi.

Posizioniamo il Firewall[1*] in modo che filtri tutti i dati di ingresso nel server DMZ[2*] dell’Applicazione Web; in questo modo tutti i potenziali input dannosi verranno analizzati e scartati.

1*Un firewall è un componente di sicurezza informatica progettato per monitorare, filtrare e controllare il traffico di rete in base a regole di sicurezza predefinite. L'obiettivo principale di un firewall è proteggere una rete o un sistema informatico da accessi non autorizzati, attacchi informatici e altri rischi per la sicurezza.

2*Un server DMZ è un server situato all'interno della DMZ (Demilitarized Zone) di una rete. La DMZ è un'area di rete intermedia tra la rete interna sicura e la rete esterna non sicura (solitamente Internet).

AZIONI PREVENTIVE



IMPATTI SUL BUSINESS

Prima di analizzare l’impatto sul business chiariamo brevemente cos’è un attacco Ddos.

Un attacco DDoS (Distributed Denial of Service) è un tipo di attacco informatico in cui un grande numero di dispositivi distribuiti in modo geografico (spesso compromessi e appartenenti a una botnet) vengono coordinati per sovraccaricare e rendere inaccessibile un servizio, un sito web o un'applicazione online. L'obiettivo principale di un attacco DDoS è saturare le risorse del bersaglio, impedendo agli utenti legittimi di accedere al servizio o di utilizzare l'applicazione.

IMPATTI SUL BUSINESS

Come da consegna sappiamo che: 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.

Possiamo calcolare quindi che: IMPATTO SUL BUSINESS = 1.500 x 10 = 15.000

dove 1.500 sono EURO che mediamente gli utenti spendono

e 10 sono i minuti di inattività della piattaforma

In conclusione l'azienda, in questo, caso ha perso 15.000 EURO per colpa dell'attacco

RESPONSE

La consegna ci avvisa che la nostra Web Application è stata infettata da un Malware, ma cos’è esattamente?

Il malware è un tipo di software malevolo progettato per danneggiare o compromettere un sistema informatico, rubare informazioni, interrompere le operazioni normali di un dispositivo o svolgere altre attività dannose senza il consenso dell'utente.

Esistono vari tipi di malware, ognuno con obiettivi diversi e metodi di diffusione. Alcuni dei tipi di malware più comuni includono:

RESPONSE

Esistono vari tipi di malware, ognuno con obiettivi diversi e metodi di diffusione. Alcuni dei tipi di malware più comuni includono:

VIRUS: Un virus è un tipo di malware che si attacca a file eseguibili e si replica quando l'utente avvia l'applicazione infetta. Può danneggiare o alterare i file e programmi esistenti.

TROJAN: Un Trojan è un tipo di malware che si presenta come un software legittimo ma contiene funzionalità malevole nascoste. I Trojan possono consentire l'accesso remoto non autorizzato al sistema, rubare informazioni o installare altri malware.

BOTNET: Una botnet è una rete di dispositivi infettati controllati da un'entità esterna (spesso un attaccante) per eseguire attività malevole in modo coordinato, come attacchi DDoS.

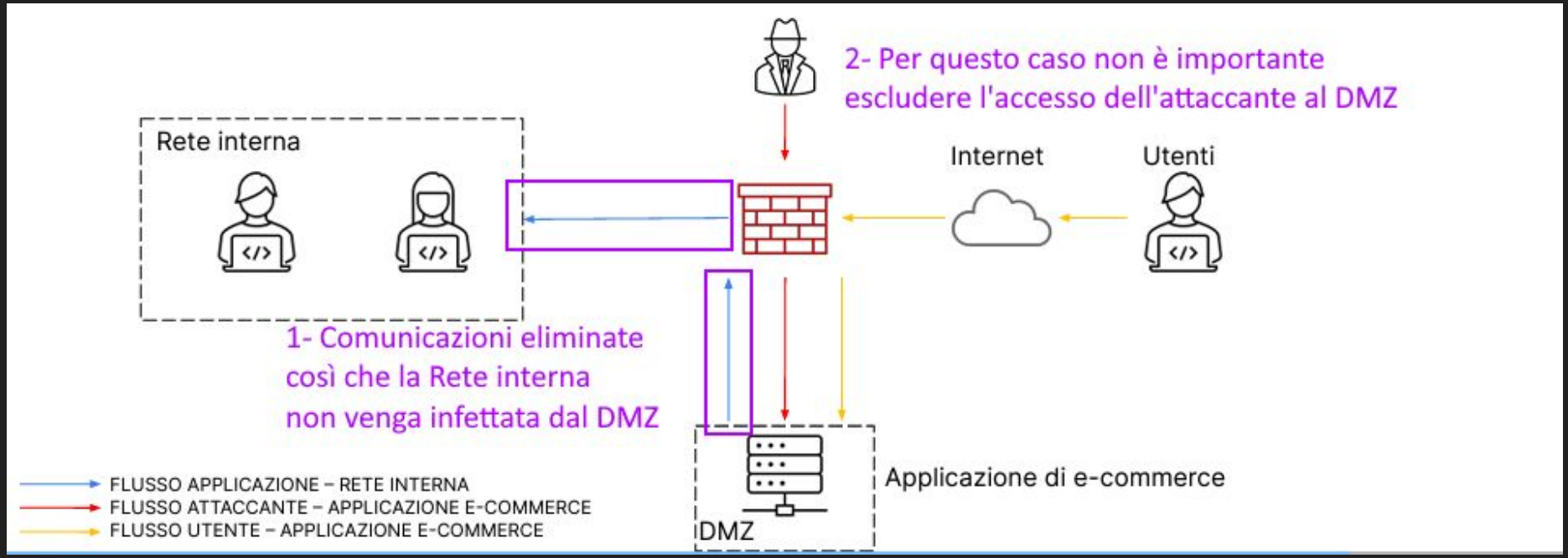
RESPONSE

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.

Per far si che il malware non si propaghi sulla nostra rete interna la prima cosa da fare è tagliare le comunicazioni tra rete interna e server DMZ; l’esercizio prosegue informandoci che non è necessario rimuovere l’accesso dell’attaccante dalla macchina interna DMZ.

Nella slide seguente è presente l’architettura modificata

RESPONSE


2- Per questo caso non è importante escludere l'accesso dell'attaccante al DMZ
Rete interna
Internet
Utenti
1- Comunicazioni eliminate così che la Rete interna non venga infettata dal DMZ
Applicazione di e-commerce
DMZ
FLUSSO APPLICAZIONE – RETE INTERNA
FLUSSO ATTACCANTE – APPLICAZIONE E-COMMERCE
FLUSSO UTENTE – APPLICAZIONE E-COMMERCE

GRAZIE