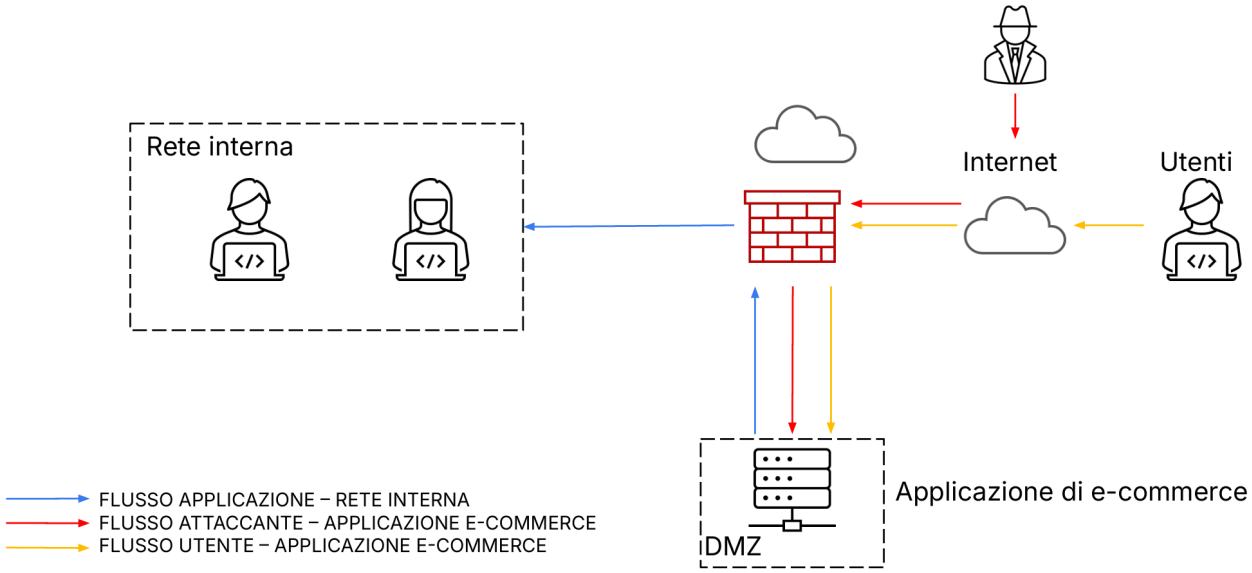
PROGETTO FINALE W20D4

TRACCIA

L'applicazione di e-commerce, raffigurata nella figura in basso, è 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, un attaccante potrebbe raggiungere la rete interna.



Con riferimento alla figura in alto, rispondere ai seguenti quesiti:

1. Quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato?

2. 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.
   Quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi DDoS?

3. L'applicazione Web viene infettata da un malware. La priorità è che non si propaghi sulla rete e non a rimuovere l'accesso da parte dell'attaccante alla macchina infettata.

4. Modifica più aggressiva dell'infrastruttura, con un budget di € 20.000/30.000, basandosi sul punto 2.

Infine, fare un disegno della soluzione completa.

SOLUZIONE

1. ATTACCO SQLi

Un attacco SQLi (Structured Query Language injection) permette a un utente non autorizzato di prendere il controllo sui comandi SQL utilizzati da un'applicazione Web (es. eliminare i dati, avere a disposizione i dati di tutti gli utenti).

Per difendere l'applicazione Web da un attacco SQLi si devono adottare le seguenti azioni preventive:

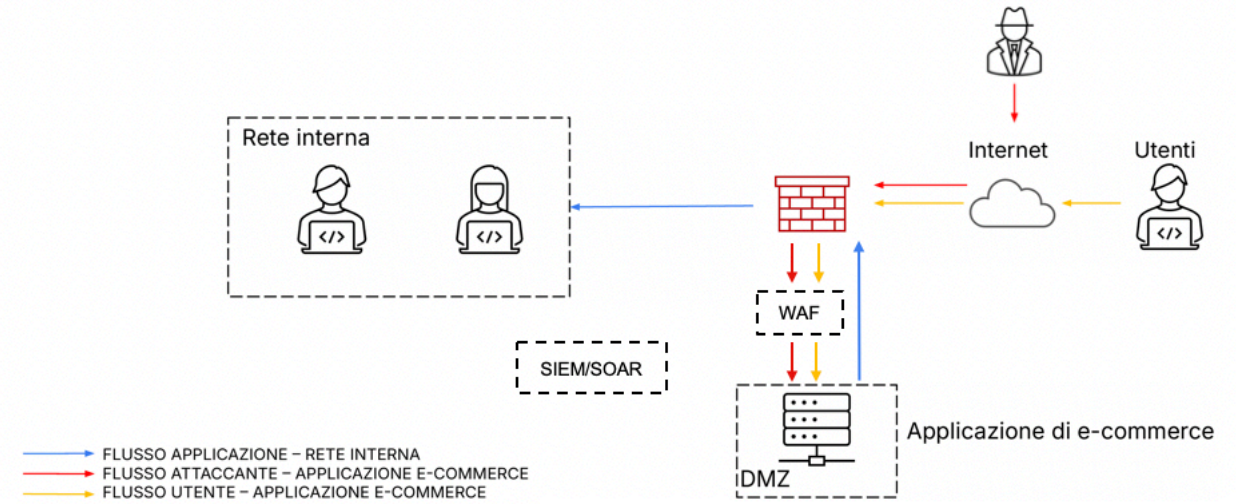
- validazione e sanificazione degli input: verificare che gli input dell'utente siano conformi ai formati attesi e rimuovere caratteri speciali
- utilizzo di istruzioni parametrizzate: dove i parametri vengono passati separatamente, impedendo al codice di interpretare i dati utente come parte della query
- monitoraggio e logging: monitorare costantemente le attività del database e registrare gli eventi sospetti per individuare e rispondere prontamente agli eventuali attacchi
- utilizzo di WAF (Web Application Firewall): aiuta a filtrare le query SQL dannose prima che raggiungano il database
- inserimento di SIEM (Security Information and Event Management): per il rilevamento e la risposta agli incidenti
- inserimento di SOAR (Security Orchestration, Automation, and Response): per una gestione e una risposta agli incidenti più efficiente e automatizzata
- limitazione dei privilegi: concedere agli utenti i minimi privilegi per interagire con il database

1. ATTACCO XSS

Un attacco XSS (Cross Site Scripting) consente all'attaccante di prendere il controllo di una applicazione Web, con gravi impatti sugli utenti che, visitando il sito web vulnerabile, subiranno le conseguenze dell'attacco (es. furto di cookie o visualizzazione di contenuti alterati).

Per difendere l'applicazione Web da un attacco XSS si devono adottare le seguenti azioni preventive:

- validazione e sanificazione degli input: verificare che gli input dell'utente siano conformi ai formati attesi e rimuovere caratteri speciali
- validazione degli output: assicurarsi che i dati provenienti dal database siano validati e formattati correttamente prima di essere presentati all'utente
- implementazione di flag HttpOnly per i cookie: per ridurre la possibilità di furto di cookie
- monitoraggio: monitorare costantemente le attività del database e registrare gli eventi sospetti per individuare e rispondere prontamente agli eventuali attacchi
- implementazione di CSP (Content Security Policy): per controllare da dove il browser può caricare script e altri contenuti, limitando l'esecuzione di codice non autorizzato
- inserimento di SIEM (Security Information and Event Management): per il rilevamento e la risposta agli incidenti
- inserimento di SOAR (Security Orchestration, Automation, and Response): per una gestione e una risposta agli incidenti più efficiente e automatizzata
- mantenere sempre aggiornato il software: per beneficiare delle correzioni di sicurezza
- eseguire test di sicurezza regolari: per identificare le vulnerabilità prima che vengano sfruttate



2. ATTACCO DDoS

In un attacco DDos (Distributed Denial of Service) l'attaccante utilizza una botnet (rete di sistemi compromessi) per inviare simultaneamente traffico dannoso al servizio di destinazione da diverse posizioni geografiche.

spesa utenti ogni minuto	€ 1.500	x
minuti di non raggiungibilità del servizio	10	=
? impatto sul business dovuto alla non raggiungibilità del servizio	€ 15.000	

La compagnia in 10 minuti ha perso 15.000 € di potenziali acquisti.

Per difendere l'applicazione Web da un attacco DDoS si devono adottare le seguenti azioni preventive:

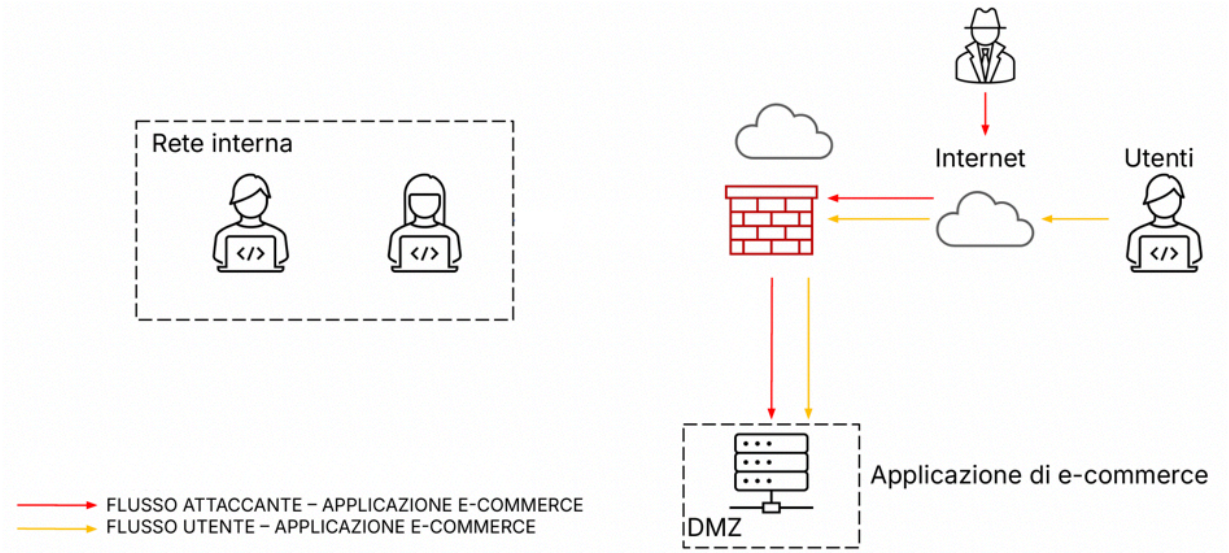
- utilizzo di WAF (Web Application Firewall): agisce come un filtro di sicurezza, analizzando il traffico in entrata e bloccando le richieste dannose
- inserimento di SIEM (Security Information and Event Management): per il rilevamento e la risposta agli incidenti
- inserimento di SOAR (Security Orchestration, Automation, and Response): per una gestione e una risposta agli incidenti più efficiente e automatizzata
- implementazione IDPS (sistemi di rilevamento e risposta alle intrusioni): monitorano costantemente la rete per attività sospette e bloccano/segnalano eventuali attacchi DDoS
- implementazione EDR (Extended Detection and Response): offre più visibilità sulle minacce
- implementazione servizi di mitigazione DDoS: monitorano il traffico in tempo reale e utilizzano tecniche avanzate per filtrare/deviare/bloccare il traffico dannoso

3. MALWARE

Un Malware (Malicious Software: virus, worm, trojan, rootkit, bootkit, backdoors, adware, spyware, dialer, keylogger, botnet) è qualsiasi software utilizzato con l'intento di procurare danni su un sistema operativo (es. causare un DoS, spiare l'attività degli utenti, avere controllo non autorizzato a dati e sistemi).

Per non far propagare il Malware sulla rete interna si devono adottare le seguenti azioni:

- isolamento della rete interna: separare la rete interna dalla DMZ (fa parte della fase di contenimento, rimozione e recupero di un incident response)
- implementazione IDPS (sistemi di rilevamento e risposta alle intrusioni): per rilevare e bloccare attività dannose sulla rete



4. MODIFICA DELL'INFRASTRUTTURA

Per rendere l'applicazione Web più sicura, si potrebbero integrare le seguenti modifiche:

AZIONE PREVENTIVA	MODIFICA AGGIUNTIVA	COSTO ANNUO
utilizzo di WAF (Web Application Firewall)	Gateway applicazione di Microsoft Azure, versione media	€ 1.000,00
inserimento del SIEM (Security Information and Event Management)	basato su cloud, per 5.000 unità di commit	€ 4.000,00
inserimento del SOAR (Security Orchestration, Automation, and Response)	funzionalità e numero di utenti medio/basse	€ 15.000,00
inserimento dell'IDPS (Intrusion Detection and Prevention System)	per piccole aziende	€ 200,00
inserimento dell'EDR (Extended Detection and Response)	per 5 utenti	€ 200,00
inserimento dei servizi di mitigazione DDoS	Microsoft Azure, per 100 risorse di indirizzo IP pubblico	€ 30,00
TOTALE		**€ 20.430,00**

SOLUZIONE COMPLETA