S9 LEZIONE 5 – PROGETTO

Traccia: rispondere ai seguenti quesiti.

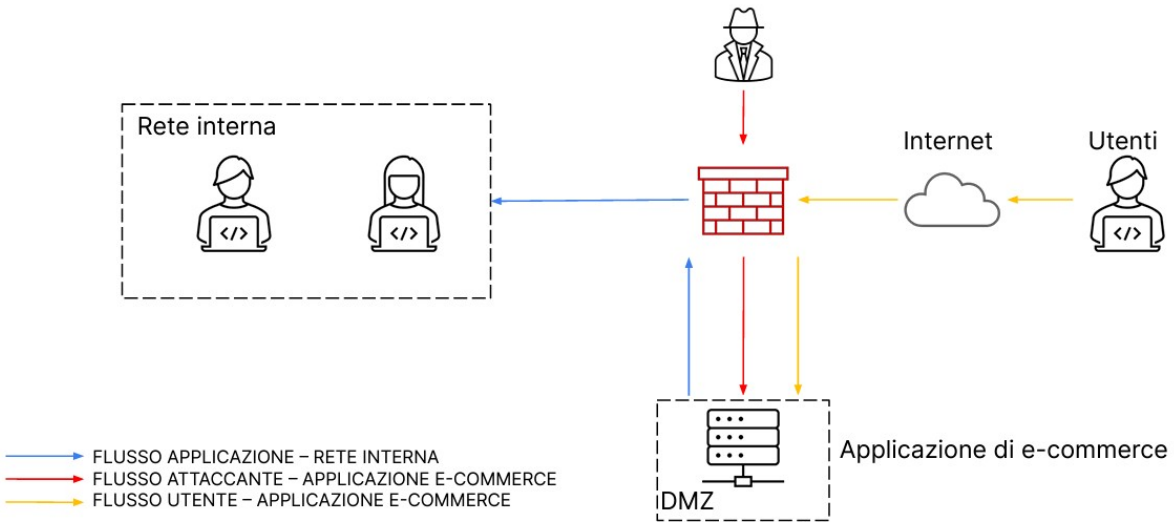
1. Azioni preventive: quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni.

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 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.



AZIONI PREVENTIVE

SQL injection (SQLi) è una vulnerabilità informatica che si verifica quando un'applicazione web accetta input utente (solitamente attraverso moduli web o parametri URL) e li incorpora direttamente nelle istruzioni SQL senza validazione o sanificazione.
Questo può consentire a un attaccante di eseguire istruzioni SQL non autorizzate nel database.
Punti chiave:

1. Input non sanificato: quando un'applicazione web accetta input utente senza validazione o sanificazione, è possibile che un attaccante possa inserire del codice SQL dannoso.

2. Incorporazione diretta nel SQL: l'input fornito dagli utenti viene incorporato direttamente nelle query.

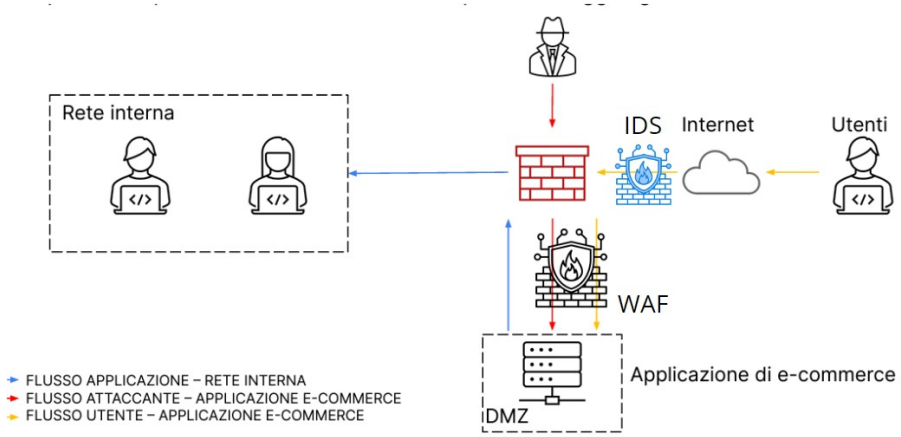
3. Esecuzione comandi dannosi: una volta che l'attaccante è in grado di inserire codice SQL dannoso, può eseguire un gran numero di operazioni come l'estrazione, la modifica o l'eliminazione di dati sensibili dal database. Inoltre può eseguire comandi che compromettono la sicurezza del sistema.

4. Potenziali danni: questi attacchi possono comportare una vasta gamma di danni, tra cui la divulgazione non autorizzata di informazioni, la compromissione dell'integrità dei dati e l'accesso non autorizzato al sistema.

Cross-Site Scripting (XSS) è una vulnerabilità di sicurezza che si verifica quando un'applicazione web permette l'inserimento di script danno si all'interno delle pagine web visualizzate dagli utenti. Gli attaccanti sfruttano questa vulnerabilità per eseguire script maligni sul browser degli utenti, compromettendo così la sicurezza dell'applicazione e mettendo a rischio i dati degli utenti.
Tipi di XSS:

1. Stored XSS: gli script dannosi sono memorizzati sul server e restituiti a tutti gli utenti che visualizzano la pagina contaminata.
2. Reflected XSS: gli script dannosi sono incorporati direttamente nell'URL e restituiti solo agli utenti che cliccano su un link contaminato. Questo tipo di XSS è spesso sfruttato attraverso attacchi di phishing.

Un metodo efficace per mitigare questo tipi di attacchi può essere l'utilizzo di un Web Application Firewall (WAF), è una soluzione di sicurezza informatica progettata per proteggere le applicazioni web da una serie di attacchi, inclusi quelli di tipo SQL injection, Cross-Site Scripting e altri exploit che mirano alle vulnerabilità web.
Un Web Application Firewall agisce come un filtro tra le richieste degli utenti e il server che ospita l'applicazione. Monitora e analizza il traffico HTTP tra l'utente e l'applicazione, identificando e bloccando eventuali attacchi o comportamenti sospetti.
Un WAF protegge l'applicazione da attacchi noti ed è in gradi di rilevare e bloccare SQL injection e Cross-Site Scripting.
Nel caso in cui l'attaccante sia esterno e passi da internet si potrebbe implementare misure difensive come IDS e IPS, i quali sono sistemi di sicurezza progettati per rilevare e prevenire intrusioni e attacchi nei sistemi informatici.



IMPATTI SUL BUSINESS A SEGUITO DEL DDoS

Il DDoS è una tipologia di attacco informatico che cerca di rendere inaccessibile un servizio, un sito web o un'applicazione, sovraccaricandola con un volume ingente di traffico proveniente da diverse fonti sulla rete.
L'obiettivo del DDoS è sovraccaricare le risorse del sistema target impedendo così agli utenti legittimi di accedere ai servizi offerti. Le fonti che lanciano questo tipo di attacchi costituiscono una botnet, ovvero un'entità complessiva governata da un attaccante. In poche parole una botnet è una vasta rete di computer compromessi usati per inviare simultaneamente richieste al bersaglio.

In questo specifico caso il DDoS rende l'applicazione non raggiungibile per 10 minuti, siccome gli utenti, secondo i calcoli, spendo 1500€ al minuto sulla piattaforma, l'impatto del business dovuto a questo attacco è di 15000€.
Questo comporta una grossa perdita per l'azienda, con l'installazione di dei sistemi di sicurezza adeguati questi danni si sarebbero potuti evitare.

POTENZIALI DANNI

Il termine "malware" è una contrazione delle parole "malicious software", che si traduce in italiano come "software maligno". Si riferisce a qualsiasi tipo di software progettato per danneggiare, alterare, o compromettere il funzionamento di un computer, una rete o un dispositivo. Il malware è creato da cybercriminali con l'obiettivo di rubare informazioni, interrompere il normale funzionamento di un sistema, o sfruttare vulnerabilità per scopi dannosi.

Ecco alcuni tipi comuni di malware:

- Virus: Si diffondono inserendosi nel codice esistente di altri programmi o file eseguibili. Una volta attivati, possono replicarsi e diffondersi ad altri file o sistemi.

- Worm: A differenza dei virus, i worm non necessitano di un file ospite per diffondersi. Si propagano autonomamente attraverso reti e dispositivi, sfruttando spesso vulnerabilità di sicurezza.

- Trojan: Si nascondono all'interno di un'apparenza innocua o legittima, ma contengono funzionalità dannose. Possono essere utilizzati per aprire una "porta segreta" nel sistema, consentendo l'accesso non autorizzato agli attaccanti.

- Spyware: Raccoglie informazioni sulle attività degli utenti senza il loro consenso. Può monitorare le attività di navigazione, raccogliere dati personali o registrare le tastate.

- Ransomware: Crittografa i dati sul computer o sulla rete della vittima, rendendoli inaccessibili. Gli autori del ransomware richiedono un riscatto in cambio della chiave di decrittazione.

Il server web dell’e-commerce è all’interno della DMZ, essa è una porzione della rete aziendale separata dal resto della LAN con il fine di ottenere un livello di sicurezza maggiore. Tuttavia, gli host presenti all’interno della parte restante di rete interna riescono a connettersi al server web.

In quanto la parte infettata è la DMZ, la prima cosa da fare è isolarla dal resto della LAN così da evitare che l’infezione si propaghi. In questo caso non si parla solo di isolamento ma di una vera e propria quarantena così da contenere prima di tutto i danni e in secondo luogo studiarne il comportamento per sviluppare strategie efficaci di prevenzione e risposta.
Attraverso il comportamento di black hat hacker, gli esperti di sicurezza informatica possono identifcare modelli e tendenze che caratterizzano gli attacchi. Per di più lo studio di queste situazioni può contribuire allo sviluppo di strumenti avanzati di sicurezza informatica.