Progetto - S9/L5

Computer Security Incident Response Team (CSIRT)

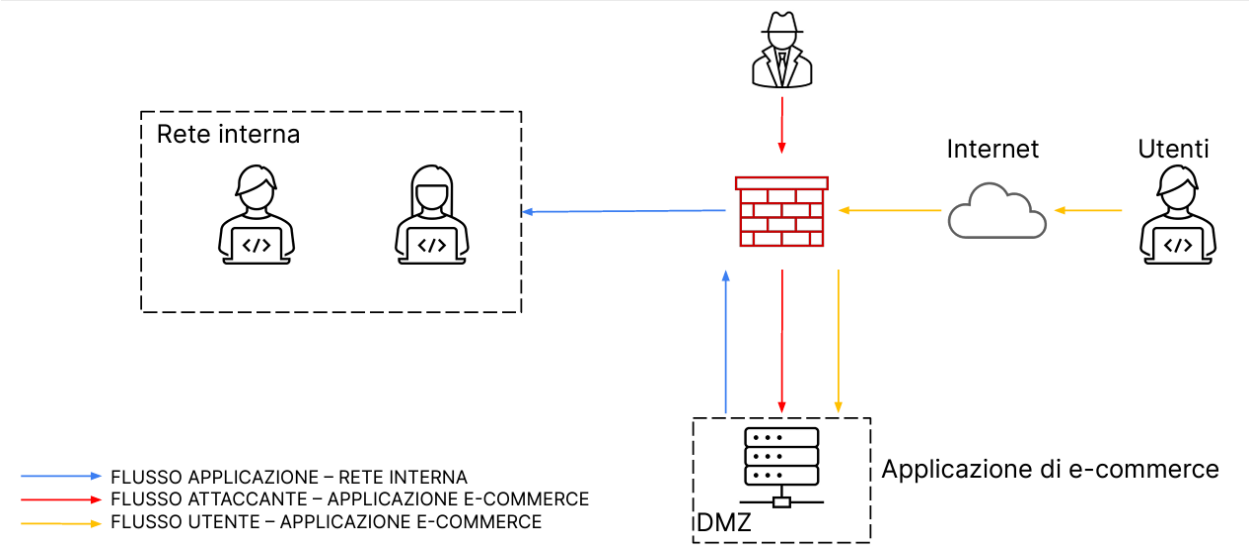
Natalino Imbrogno

Cybersecurity Specialist

EPICODE

OBIETTIVO

Si ha la seguente situazione



Un'azienda che gestisce una web application di ecommerce intende implementare azioni preventive al fine di difendere il proprio servizio da attacchi di tipo SQLi oppure XSS da parte di una o più possibili persone malintenzionate.

Inoltre, la web app subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione non raggiungibile per 10 minuti. Viene richiesto, a tal proposito, di calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio considerando che in media ogni minuto gli utenti spendono 1500€ sulla piattaforma di ecommerce.

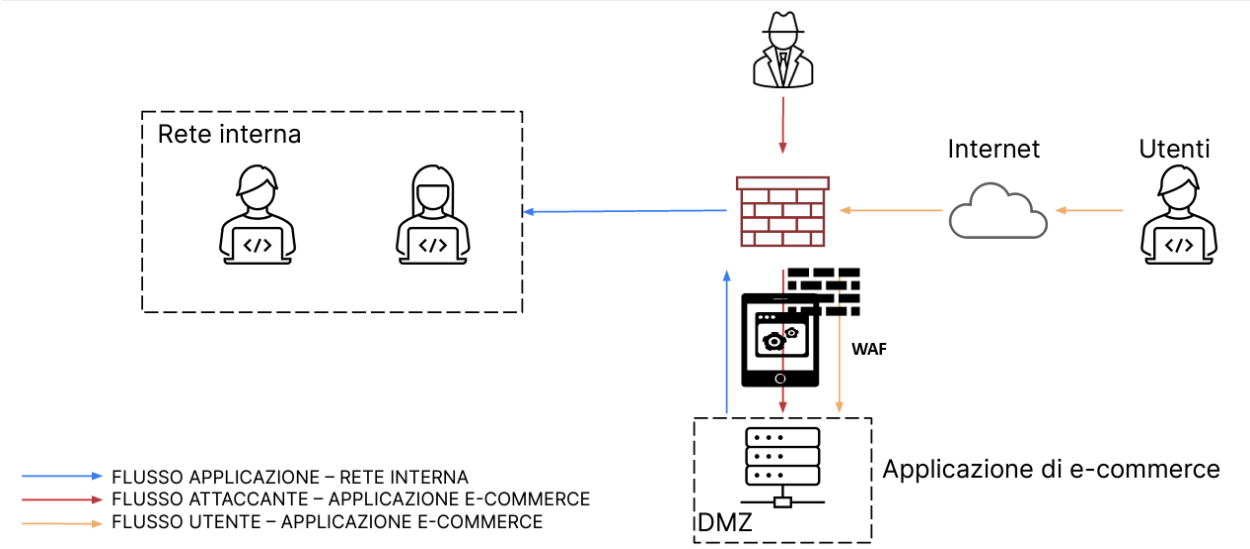
Come se non bastasse, l'applicazione web viene infettata da un malware. La priorità è che il malware non si propaghi sulla rete interna aziendale, mentre non è richiesto rimuovere l'accesso da parte dell'attaccante alla macchina infettata, sia perché l'applicazione di ecommerce deve essere disponibile per gli utenti/clienti tramite internet, ma anche per studiare il comportamento dell'attaccante.

AZIONI PREVENTIVE

L'SQLi è una tecnica di attacco informatico che sfrutta le vulnerabilità presenti all'interno delle web app che utilizzano database per la gestione dei dati. Dato che SQL è un linguaggio di interrogazione utilizzato per interagire con il database, l'SQLi sfrutta le debolezze nella gestione delle query SQL all'interno dell'applicazione.

L'XSS, invece, è un tipo di attacco informatico che si verifica quando un'applicazione web permette ad una o più persone malintenzionate di iniettare script dannosi all'interno delle pagine visualizzate da altri utenti. Gli attacchi XSS, dunque, sfruttano la fiducia che un utente ha nell'applicazione e nei dati che vengono visualizzati dal browser. Esistono diverse tipologie di XSS, ma in generale, l'obiettivo principale è eseguire script lato client nel browser della vittima.

A tal proposito, l'utilizzo di un Web Application Firewall (WAF) può essere un metodo efficace per mitigare questo tipo di attacchi. Un WAF è un dispositivo o un'applicazione software che monitora, filtra e blocca il traffico HTTP in ingresso e in uscita tra un'applicazione web e internet. Esso, pertanto, può essere configurato per rilevare pattern di query SQL malevole e bloccare le richieste prima che raggiungano il server web. E anche per quanto riguarda l'XSS, esso può rilevare e bloccare script dannosi all'interno del traffico HTTP in ingresso, impedendo che tali script raggiungano il browser dell'utente.



IMPATTI SUL BUSINESS A SEGUITO DEL DDOS

Il DDoS è una tipologia di attacco informatico mirato a rendere inaccessibile un servizio, un sito web o un'applicazione, sovraccaricandolo con un volume massiccio di traffico proveniente da diverse fonti distribuite in rete. L'obiettivo di un attacco DDoS è sopraffare le risorse del sistema target impedendo agli utenti legittimi di accedere ai servizi offerti. Le fonti che lanciano l'attacco costituiscono una botnet, ovvero un'entità complessiva governata da un cosiddetto botmaster. Quest'ultimo può essersi procurato gli host zombie della botnet o affittandoli sul dark web, o infettando i dispositivi di utenti ignari, oppure magari si è in presenza di una vera e propria organizzazione attrezzata a dovere. Inoltre, il botmaster, se sa il fatto suo, riesce a controllare i suoi zombie grazie ad un server remoto noto come control and command server (C&C o C2). Il server fornisce un vero e proprio canale di comunicazione attraverso il quale l'attaccante può inviare comandi agli host della botnet e ricevere dati da essi.

Nel caso specifico dell'azienda presa in esame, il DDoS rende l'applicazione non raggiungibile per 10 minuti, e siccome gli utenti spendono 1500€/minuto sulla piattaforma, l'impatto del business dovuto alla non raggiungibilità del servizio è 15000€. Perciò si può concludere che l'entità del danno causato da questo attacco, in termini economici, equivale quantitativamente alla somma appena calcolata.

CONTENIMENTO DELL'INFEZIONE DA MALWARE

Un malware è qualsiasi tipo di software progettato per danneggiare, infiltrarsi o compromettere un sistema informatico senza il consenso dell'utente. Esso può assumere diverse forme e svolgere una varietà di funzioni malevole, inclusa la raccolta di informazioni sensibili, il danneggiamento dei dati, il controllo remoto di un sistema o la distribuzione di ulteriori malware. Tra le categorie di malware più comuni, possiamo annoverare:

- il virus, ovvero un tipo di malware che si attacca a file eseguibili o a settori di avvio di dispositivi di archiviazione e si replica quando questi file vengono eseguiti o i dispositivi vengono avviati;
- il worm, e cioè un malware autonomo che si replica automaticamente e si diffonde attraverso le reti, sfruttando spesso delle vulnerabilità di sicurezza per infettare i sistemi senza l'intervento dell'utente;

- il trojan, che sarebbe un programma dannoso mascherato da software legittimo. Una volta installato, può eseguire azioni dannose come la raccolta di informazioni, l'apertura di una backdoor nel sistema o la distribuzione di altri malware;
- lo spyware, ovvero un malware progettato per raccogliere informazioni sulle attività degli utenti senza il loro consenso. Può monitorare la navigazione web, registrare ciò che viene digitato sulla tastiera o raccogliere dati personali;
- l'adware, e cioè un malware progettato per visualizzare annunci pubblicitari indesiderati sul computer dell'utente, spesso con il fine di generare entrate per gli autori del malware stesso;
- il ransomware, che crittografa i dati sul sistema della vittima e richiede un riscatto per fornire la chiave di decrittazione;
- il rootkit, ovvero un insieme di programmi e strumenti progettati per ottenere e mantenere l'accesso non autorizzato ad un sistema, spesso mascherando la sua presenza o attività.

Passiamo ora all'azienda presa in considerazione.

Il server web del portale di ecommerce sta all'interno della DMZ. Quest'ultima 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 restante fetta di rete interna riescono comunque a connettersi al web server.

Nel momento in cui esso viene infettato, per contenere il danno, la prima cosa da fare è isolare la DMZ dal resto della LAN, così da impedire che l'infezione si propaghi.

Inoltre, in questo caso specifico, non parliamo di semplice isolamento, bensì di vera e propria quarantena per il web server, dato che è opportuno, oltre al contenimento dell'incidente di sicurezza, sul piano informativo, monitorare e analizzare il comportamento dell'attaccante così da imparare a sviluppare strategie più efficaci di prevenzione e risposta.

Infatti, attraverso il comportamento dei criminali informatici, gli esperti di sicurezza possono identificare modelli e tendenze che caratterizzano gli attacchi. Inoltre, lo studio dell'attaccante può contribuire allo sviluppo di strumenti avanzati di sicurezza informatica, come sistemi di rilevamento delle minacce più sofisticati, analisi comportamentali degli utenti e sistemi di intelligenza artificiale per il rilevamento delle anomalie. Infine, questa tipologia di analisi è utile anche per la formazione degli esperti di sicurezza e per aumentare la consapevolezza tra gli utenti finali.

Quindi la DMZ non può essere rimossa eliminando la sua connessione con internet sia per il motivo appena illustrato, e sia perché altrimenti tutti i servizi destinati al cliente finale cesserebbero di essere erogati. L'azienda, ovviamente, dopo un'attenta ed accurata analisi, si è resa conto che i costi relativi alla messa offline della piattaforma di ecommerce sarebbero maggiori rispetto all'eventuale danno di immagine causato da un'infezione molto più estesa che partirebbe da tutti gli utenti che si connettono al sito.