Report sulla Sicurezza delle Web App e Incident Response

Data 02/02/24

Indice

Introduzione

Nell'era digitale, la sicurezza delle Web App è di primaria importanza data la crescente minaccia di attacchi come SQL Injection (SQLi) e Cross-Site Scripting (XSS). Questo report si focalizzerà sulle azioni preventive implementate in risposta a una richiesta specifica sull'applicazione Web. Successivamente, si affronterà la gestione di un attacco DDoS e di un'infezione da malware. In aggiunta, verranno fornite brevi nozioni teoriche sull'Incident Response e sulle politiche adottate in situazioni simili.

Incident Response e Politiche di Sicurezza

L'Incident Response è una disciplina che si occupa della gestione degli incidenti di sicurezza, comprese le minacce informatiche. In situazioni di attacco, una corretta risposta è cruciale. Le politiche di sicurezza dovrebbero definire chiaramente i passaggi da intraprendere per identificare, contenere, eradicare e recuperare da un incidente. L'adozione di playbooks specifici per tipologie di attacco, come SQL Injection o XSS, facilita una risposta efficace. Le politiche devono anche contemplare il coinvolgimento delle autorità competenti e la comunicazione trasparente con gli stakeholder.

Azioni Preventive contro SQLi e XSS

La richiesta di esercizio chiedeva quali azioni preventive implementereste per difendere l’applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato.

Esempi di azioni preventive contro SQLi e XSS

La prevenzione di attacchi SQLi e XSS richiede l'adozione di misure efficaci per neutralizzare le vulnerabilità associate a tali minacce. Tecniche preventive possono includere:

Validazione Input: Verifica e validazione rigorosa di tutti i dati in ingresso per prevenire l'inserimento di comandi malevoli.

Uso di Parametrized Statements: L'utilizzo di dichiarazioni parametriche nelle query SQL aiuta a separare i dati utente dai comandi SQL, riducendo il rischio di SQL Injection.

Controllo dei Cookie e Header HTTP: Monitoraggio e filtraggio attivo di cookie e header HTTP per mitigare attacchi XSS basati su iniezioni di script.

Implementazione di Content Security Policy (CSP): L'uso di CSP consente di limitare l'esecuzione di script a origini specifiche, riducendo il rischio di XSS.

Implementazione di un WAF (Web Application Firewall): L'implementazione di un WAF fornisce un ulteriore strato di difesa per le applicazioni web, contribuendo a prevenire violazioni della sicurezza e a proteggere i dati sensibili dagli attacchi informatici.

Scelta di Web Application Firewall (WAF)

Di fronte alla richiesta di adottare azioni preventive contro SQLi e XSS, è stata presa la decisione di implementare un Web Application Firewall (WAF).

Un Web Application Firewall (WAF) è una soluzione di sicurezza proattiva progettata per proteggere le applicazioni web da una vasta gamma di attacchi informatici. Operando come uno scudo tra le applicazioni web e il traffico in ingresso, il WAF analizza e filtra le richieste HTTP in tempo reale per identificare e bloccare potenziali minacce. Utilizza regole predefinite o personalizzate per rilevare e mitigare attacchi comuni come SQL Injection (SQLi), Cross-Site Scripting (XSS), e altri exploit web.

Le principali funzionalità di un WAF includono:

Filtraggio delle Richieste: Analizza le richieste in ingresso, filtrando e bloccando quelle che potrebbero costituire una minaccia.

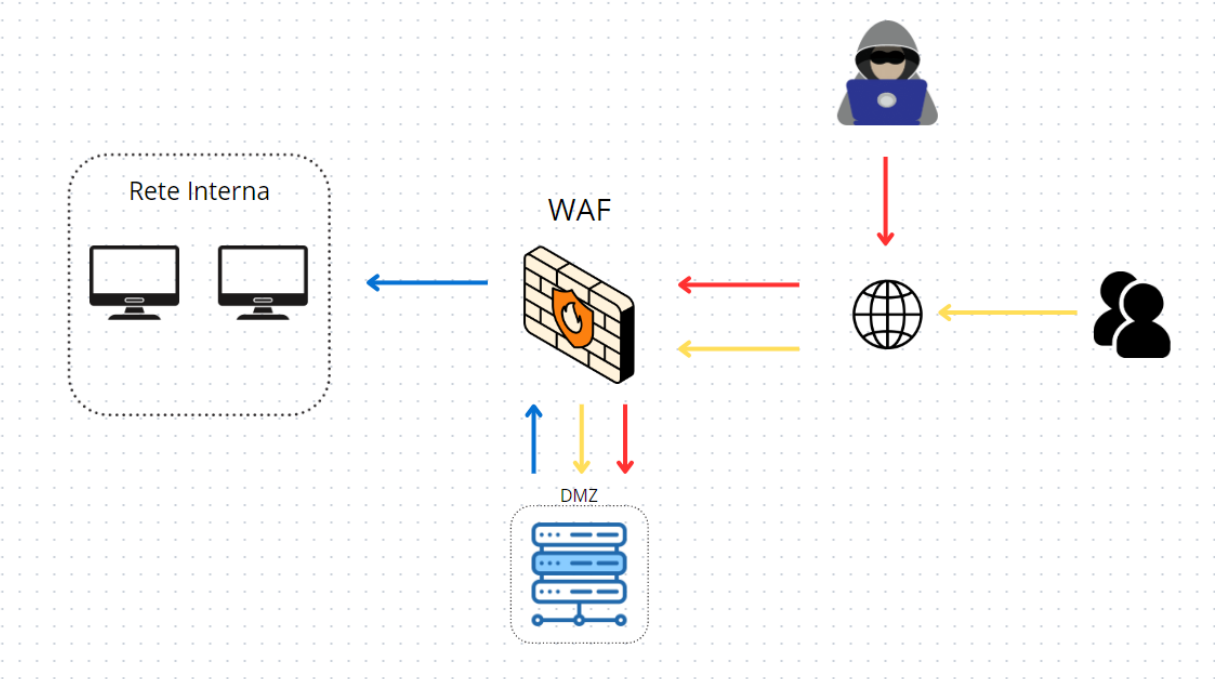
Validazione degli Input: Controlla e valida i dati in ingresso per prevenire attacchi che sfruttano vulnerabilità come SQLi.

Rilevamento delle Anomalie: Monitora il traffico per identificare modelli anomali o comportamenti sospetti che potrebbero indicare un attacco.

Protezione contro Attacchi XSS: Identifica e blocca tentativi di Cross-Site Scripting, un attacco in cui script dannosi vengono eseguiti sul browser dell'utente.

Controllo delle Sessioni: Gestisce le sessioni utente e rileva attività sospette, come tentativi di session hijacking.

Protezione contro Attacchi DDoS: Alcuni WAF includono funzionalità per mitigare attacchi Distribuited Denial of Service (DDoS), proteggendo l'infrastruttura da sovraccarichi di traffico.



Impatto del DDoS sulla Web App

Attacco DDoS

Un attacco DDoS (Distributed Denial of Service) mira a rendere un servizio, come una Web App, inaccessibile ai legittimi utenti sovraffollando il servizio con un volume anomalo di traffico. Questo può essere ottenuto attraverso l'uso di una rete distribuita di dispositivi compromessi (botnet) che inviano richieste al servizio bersaglio in modo simultaneo, saturandone le risorse e impedendo l'accesso a utenti legittimi. Gli attacchi DDoS possono causare interruzioni temporanee o prolungate dei servizi, danneggiando l'accessibilità e la reputazione dell'organizzazione.

Danni Causati da un Attacco DDoS:

Interruzione del Servizio: L'obiettivo primario di un attacco DDoS è interrompere la normale erogazione di servizi, rendendo le risorse inaccessibili per un periodo di tempo variabile.

Perdita di Fatturato: L'interruzione delle operazioni online può comportare la perdita di opportunità di vendita e transazioni, influenzando negativamente il fatturato.

Danno Reputazionale: Gli utenti insoddisfatti a causa dell'indisponibilità del servizio possono riflettersi negativamente sulla reputazione dell'organizzazione.

Costi Operativi Aggiuntivi: La mitigazione di un attacco DDoS può richiedere risorse aggiuntive, aumentando i costi operativi.

Analisi dell'impatto economico

L'analisi prosegue affrontando una situazione di attacco DDoS che rende l'applicazione non raggiungibile per 10 minuti, considerando che in media ogni minuto gli utenti spendono 1.500 € sulla piattaforma di e-commerce.

Il calcolo dell'impatto finanziario sulla base della spesa media degli utenti per minuto (1.500€) di conseguenza abbiamo utilizzato il seguente calcolo per stabilire la perdita totale durante i 10 min di interruzione del servizio:

Impatto = 1.500 € x 10 minuti = 15.000 €

Questa valutazione evidenzia l'importanza di implementare misure di difesa avanzate contro attacchi DDoS per garantire la continuità operativa e mitigare perdite finanziarie.

Gestione di un Attacco da Malware

In una situazione di attacco da malware, è essenziale adottare misure immediate per limitare i danni e prevenire la propagazione dell'infezione. Tecniche comuni in Incident Response includono l'isolamento del sistema infetto, la rimozione del sistema e tecniche come il “Purge” e il “Destroy”.

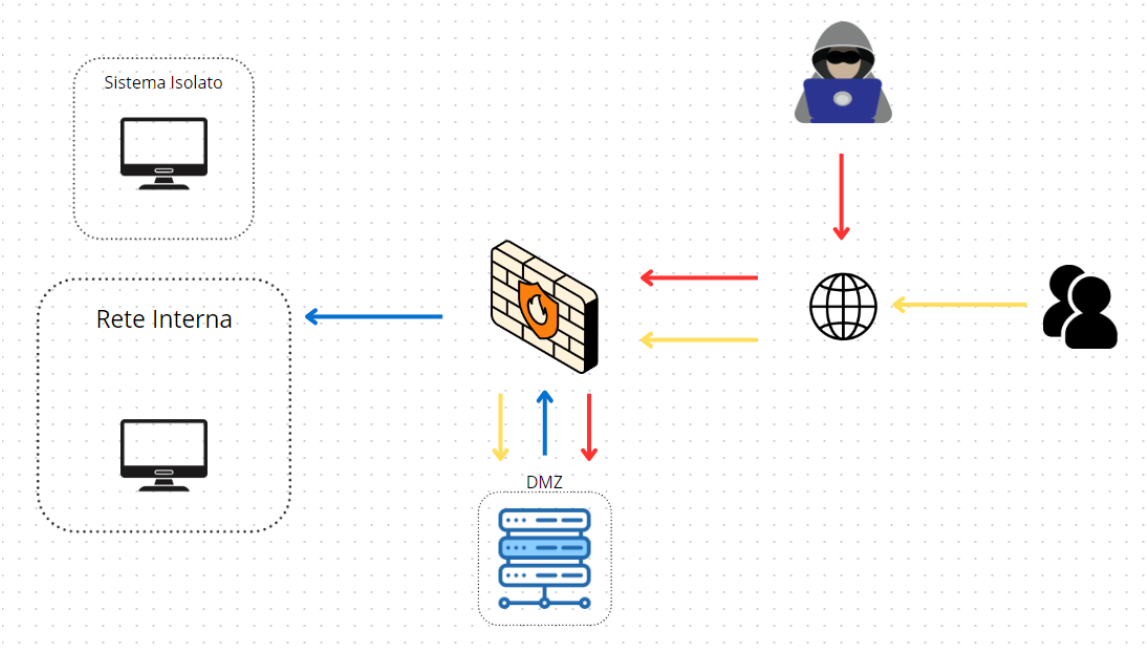
L'isolamento è spesso la prima risposta per impedire la contaminazione di altri sistemi, garantendo che il malware non possa propagarsi attraverso la rete. La rimozione del sistema infetto può includere la disinfezione delle risorse colpite o, in casi estremi, la sostituzione del sistema compromesso.

Decisione di Isolare la Macchina Infetta

Nel caso specifico descritto nel report, l'isolamento è stato implementato con un focus particolare sulla rapida attuazione. La macchina infetta è stata disconnessa dalla rete interna e da internet.

Questa decisione è stata presa per evitare che il malware si diffondesse attraverso la rete aziendale.

L'isolamento, se attuato prontamente, rappresenta un mezzo efficace per bloccare la progressione dell'attacco, consentendo al team di sicurezza di concentrarsi sulla successiva fase di risposta. È fondamentale accompagnare l'isolamento con un'analisi forense approfondita per identificare il malware, gli artefatti correlati e le possibili vie di ingresso. Questa approfondita analisi è essenziale per garantire che ogni traccia dell'attacco sia completamente eliminata, riducendo al minimo il rischio di reinfezione e preservando eventuali prove digitali utili per ulteriori indagini.



Conclusioni

Nel contesto sempre più complesso della sicurezza informatica, la protezione delle Web App assume un ruolo centrale nella difesa contro una vasta gamma di minacce, tra cui SQL Injection (SQLi), Cross-Site Scripting (XSS), attacchi DDoS e infezioni da malware. Questo report ha esaminato le azioni preventive adottate in risposta a una richiesta specifica, affrontando poi situazioni di attacco DDoS e malware.

Incident Response e Politiche di Sicurezza:

La gestione degli incidenti di sicurezza richiede una risposta tempestiva e coordinata. L'Incident Response, disciplina chiave in questo contesto, si concentra sull'identificazione, contenimento, eradicazione e recupero da un attacco. Le politiche di sicurezza dovrebbero essere robuste e comprendere playbooks specifici per tipologie di attacco, garantendo il coinvolgimento delle autorità competenti e una comunicazione trasparente con gli stakeholder.

Azioni Preventive contro SQLi e XSS:

La prevenzione di attacchi SQLi e XSS è fondamentale per mitigare rischi associati a vulnerabilità nelle applicazioni web. L'adozione di pratiche come la validazione rigorosa degli input, l'uso di dichiarazioni parametriche nelle query SQL, il controllo attivo dei cookie e header HTTP, l'implementazione di Content Security Policy (CSP) e l'adozione di un Web Application Firewall (WAF) sono passi chiave per fortificare la difesa delle Web App.

Impatto del DDoS sulla Web App:

Gli attacchi DDoS, volti a sovraccaricare le risorse di una Web App, possono causare danni significativi, inclusi l'interruzione del servizio, la perdita di fatturato, il danno reputazionale e costi operativi aggiuntivi. L'analisi dell'impatto economico nel nostro caso specifico ha sottolineato l'importanza di misure di difesa avanzate per garantire la continuità operativa e mitigare perdite finanziarie.

Gestione di un Attacco da Malware:

La risposta a un attacco da malware richiede azioni immediate e mirate. L'isolamento della macchina infetta è spesso la prima mossa per prevenire la propagazione del malware. Nel nostro caso, la decisione di isolare la macchina infetta è stata presa per limitare danni e prevenire la diffusione dell'infezione all'interno della rete interna.

In conclusione, la sicurezza delle Web App richiede un approccio olistico, integrando azioni preventive, risposte rapide agli incidenti e politiche di sicurezza ben definite. La comprensione delle minacce e l'adozione di misure proattive sono fondamentali per mantenere la sicurezza delle applicazioni web in un ambiente sempre più sfidante e dinamico.