Security Operation

Progetto M5-W20D4

Natalia Zanghì

Versione 1.0

03/02/2025

Esercizio Traccia e requisiti

Con riferimento alla figura in slide 2, 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

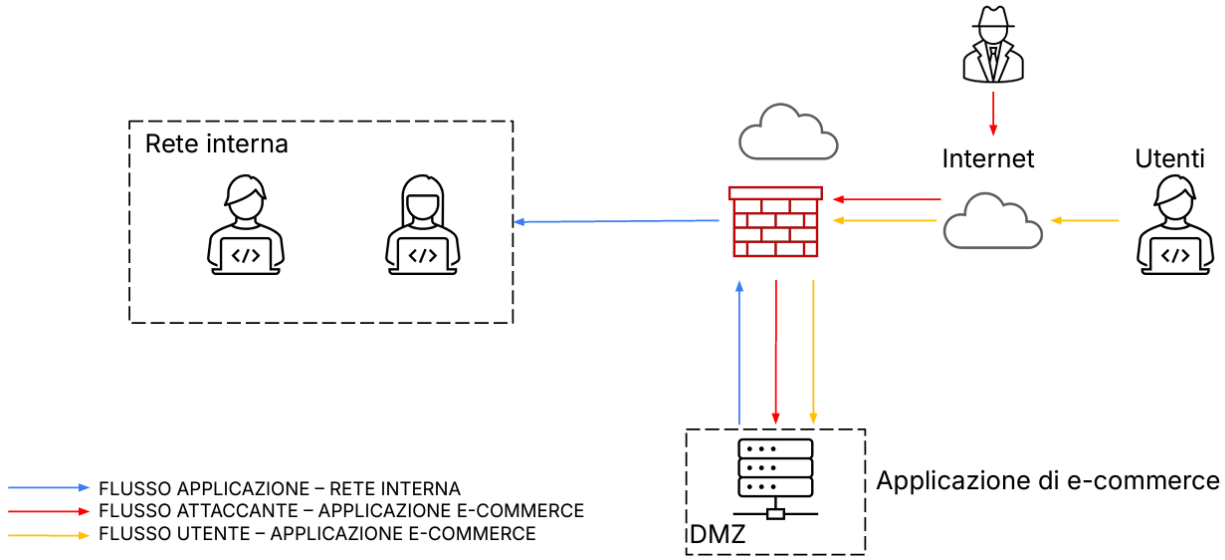
2. Impatti sul business: l'applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione non raggiungibile per 10 minuti. Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media ogni minuto gli utenti spendono 1.500 € sulla piattaforma di e-commerce. Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica

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.

4. Soluzione completa: unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)

5. Modifica «più aggressiva» dell'infrastruttura (se necessario/facoltativo magari integrando la soluzione al punto 2)

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.



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?

Per proteggere un'applicazione web da attacchi SQLi e XSS, è essenziale adottare misure preventive mirate a ridurre i rischi derivanti da queste vulnerabilità. L'attacco SQL Injection sfrutta le lacune nei moduli di input per manipolare le query al database, consentendo agli attaccanti di accedere o modificare dati sensibili. Al contrario, l'attacco Cross-Site Scripting inietta codice JavaScript dannoso in una pagina web, mettendo a rischio la sicurezza dell'utente e la protezione dei dati. Entrambi gli attacchi mirano a sfruttare debolezze nella sicurezza delle applicazioni web, con potenziali gravi conseguenze per la privacy e la protezione dei dati. Per difendersi da queste minacce, è necessario implementare una serie di misure preventive che rafforzano la sicurezza e garantiscono la protezione dei dati. Di seguito, esploreremo nel dettaglio le soluzioni più efficaci per prevenire SQLi e XSS

Misure preventive contro SQLi

Per prevenire gli attacchi SQLi , bisogna innanzitutto utilizzare la parametrizzazione delle query. Ovvero, separiamo i dati immessi dall'utente dal codice SQL, evitando che eventuali input dannosi vengano eseguiti come codice. Utilizziamo una query parametrica dove i segnaposto “ ? “ indicano dove andranno i valori di username e password. Questo garantisce che i dati vengano trattati solo come valori, non come parte del comando SQL.
Successivamente dobbiamo validare l'input. Assicuraci che i dati immessi dagli utenti siano corretti e sicuri, come verificare che un'email contenga solo caratteri validi o limitare la lunghezza degli input per prevenire comandi pericolosi.
Un altra azione utile è l’uso dei permessi minimi. Ogni utente del sistema dovrebbe avere solo i permessi necessari per il suo ruolo. Ad esempio, se un utente deve solo leggere i dati, non deve avere permessi per modificarli o cancellarli.
Abbiamo bisogno di un Web Application Firewall (WAF) per filtrare il traffico

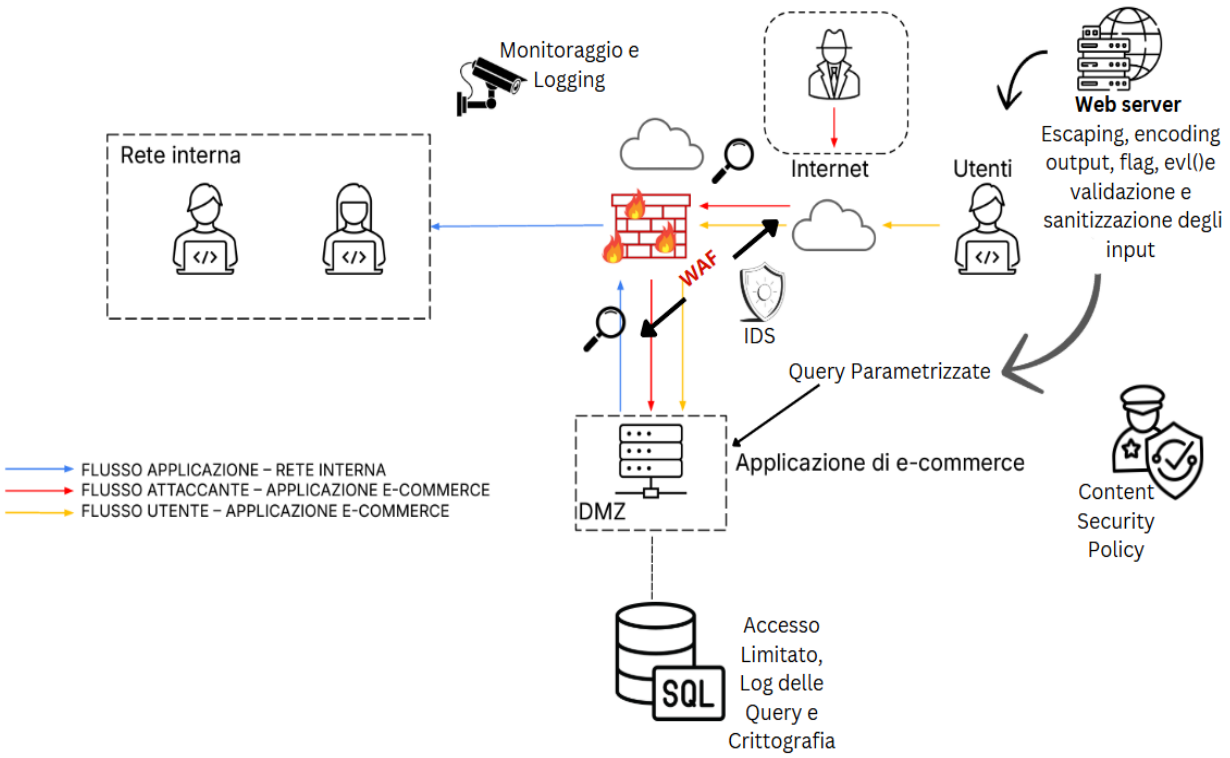
sospetto e bloccare le richieste potenzialmente pericolose, come quelle che contengono parole chiave come "SELECT" o "DROP" che potrebbero indicare un tentativo di SQL.
Crittografare i dati sensibili. Usando HTTPS per proteggere i dati durante la trasmissione e il riposo nel database, così che anche se qualcuno riesce ad accedere ai dati, non possa leggerli facilmente.
Infine, è utile implementare monitoraggio e logging per rilevare attività sospette e intervenire tempestivamente. Registrando le query e analizzando i log, è possibile individuare rapidamente potenziali attacchi.
In questo modo, garantiamo la sicurezza dei dati e limitiamo i rischi.

Misure preventive contro XSS

Per proteggersi dagli attacchi XSS, è fondamentale seguire alcune misure chiave. La codifica dell'output assicura che i dati inviati al browser siano trattati come testo, evitando che script dannosi vengano eseguiti. Ad esempio, un input come <script>alert('XSS');</script> verrà visualizzato come testo, non come codice eseguibile.
Un altro aspetto è validare gli input degli utenti per garantire che siano nel formato corretto e privi di elementi pericolosi, come caratteri speciali. La gestione dei caratteri speciali e l'uso di tecniche di escaping (ad esempio, trasformare < in <) impedisce che vengano interpretati come parte del codice HTML o JavaScript.Per aumentare la sicurezza, è consigliabile evitare funzioni rischiose come eval() e preferire alternative sicure come JSON.parse().In sintesi, queste pratiche sono parte integrante di una solida architettura di sicurezza per le applicazioni web, e rientrano nel concetto più ampio di "difesa per design", dove la sicurezza è incorporata fin dalla progettazione dell'applicazione.
Per quanto riguarda la sicurezza dei cookie, essi devono essere protetti con i flag HTTP-only (per impedire l'accesso tramite JavaScript) e Secure (per garantire che siano inviati solo su connessioni HTTPS).
Infine, una Content Security Policy (CSP) aiuta a limitare le risorse che possono essere caricate, proteggendo ulteriormente l'applicazione da script non autorizzati e attacchi XSS. Queste misure, integrate correttamente, costituiscono una solida architettura di sicurezza per le applicazioni web.

Protezione dagli Attacchi SQLi e XSS

Le iniezioni SQL (SQLi) e il Cross-Site Scripting (XSS) rappresentano attacchi mirati rispettivamente ai database e agli utenti delle applicazioni web. Sebbene si tratti di minacce distinte, entrambe possono essere fronteggiate attraverso l'implementazione di strategie simili, quali la validazione dei dati in ingresso, l'adozione di query parametrizzate, l'uso di un Web Application Firewall (WAF), l'escaping dei caratteri speciali e l'implementazione di una Content Security Policy (CSP). Attraverso l'adozione di queste soluzioni, è possibile garantire la sicurezza delle applicazioni web e proteggere i dati sensibili.



Rappresentazione grafica sull’implementazione di pratiche di sicurezza contro SQLi e XSS

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. Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica

In caso di un attacco DDoS che rende l'applicazione web di e-commerce inaccessibile per 10 minuti, è possibile calcolare l'impatto economico sulla base della spesa media per utente al minuto. Per fare ciò, utilizziamo la formula SLE (Single Loss Expectancy).

La SLE (Single Loss Expectancy) rappresenta la perdita economica attesa per un singolo evento di interruzione o attacco. La formula per calcolare la SLE è :

SLE=AV×EF×Tempo di Inattivita

// IPOTIZZANDO 8 ORE DI LAVORO.

Parametri in nostro possesso:

AV (Asset Value): 1500 euro/minuto (spesa media degli utenti per minuto)

AV = 1500 x 60 x 8 = 720K

EF = 10/ 480 = 2.08%

EF (Exposure Factor): (2.08%) - Questo valore indica una perdita parziale, in quanto il sito non genera entrate durante l'interruzione del servizio.

Tempo di Inattività: 10 minuti

SLE = 720K x 0.0208 = 14.976

Utilizzando questi parametri, il calcolo della SLE è di **14.976 euro**

Quindi se l'e-commerce risulta completamente non accessibile per 10 minuti, la perdita economica totale sarà più o meno di 15.000 euro.

Azioni preventive contro attacchi DDoS

Per proteggere un’azienda dagli attacchi DDoS e ridurne al minimo il rischio e l’impatto, è fondamentale adottare strategie preventive efficaci. Tra le prime iniziative da attuare vi è il bilanciamento del carico**,** una pratica che distribuisce il traffico su molteplici server, prevenendo il sovraccarico di un singolo server e contribuendo a mantenere la disponibilità dei servizi in caso di attacco. In questo modo, si riduce il rischio di downtime, che potrebbe compromettere la continuità operativa.
Un ulteriore strumento importante è rappresentato dal firewall per applicazioni web (WAF), che ha la funzionalità di filtrare e bloccare il traffico dannoso prima che esso raggiunga l'infrastruttura aziendale. Questo sistema è particolarmente efficace nel prevenire attacchi a livello applicativo, spesso al centro degli attacchi DDoS rivolti a saturare i server web. L'implementazione di una Content Delivery Network (CDN) costituisce un'altra strategia vantaggiosa, poiché distribuisce il traffico su server globali, riducendo l'impatto di un attacco DDoS concentrato su un singolo punto della rete. La CDN funge da barriera supplementare, assorbendo e reindirizzando il traffico malevolo lontano dai server principali.
Inoltre, per una protezione mirata, è essenziale adottare soluzioni in tempo reale per la rilevazione e la mitigazione degli attacchi DDoS. Tecnologie come sistemi IDS/IPS**,** firewall avanzati**,** centri di scrubbing**,** rate limiting e integrazione con Threat Intelligence consentono di identificare rapidamente il traffico anomalo e di bloccarlo, riducendo notevolmente i danni.
Infine, una preparazione adeguata attraverso piani di risposta è essenziale. Creare e testare piani di Business Continuity (BC) e Disaster Recovery (DR) aiuta a ridurre i tempi di inattività e a ripristinare velocemente i servizi. Questi piani assicurano che l'organizzazione sia pronta a reagire tempestivamente in caso di attacco, garantendo la continuità delle operazioni e la sicurezza complessiva dell'infrastruttura.
Attraverso l'adozione di queste misure preventive, un'azienda può mitigare significativamente i rischi associati agli attacchi DDoS e potenziare la propria resilienza operativa.

Considerazioni Qualitative

Analizzare le conseguenze qualitative di un attacco DDoS è essenziale per comprenderne l'impatto su un'azienda e i suoi clienti. Oltre agli aspetti tecnici, occorre considerare come l'attacco influenzi l'efficienza operativa, la reputazione e la fiducia dei clienti. Un DDoS può danneggiare seriamente l'immagine dell'azienda, portando i clienti a perdere fiducia e a rivolgersi alla concorrenza. Per questo motivo, garantire un sito web sicuro e affidabile è fondamentale. Dopo l'attacco, è importante ripristinare rapidamente il servizio, rispondere alle domande dei clienti e affrontare eventuali implicazioni legali. Un'interruzione del servizio può ostacolare le operazioni quotidiane, riducendo la produttività e influenzando negativamente dipendenti e fornitori. Pianificare in anticipo permette di ristabilire rapidamente la fiducia dei clienti, limitando i danni e proteggendo tanto l'efficienza operativa quanto la reputazione aziendale.

Conclusione

Un piano solido di Business Continuity e Disaster Recovery è essenziale per rispondere rapidamente a un attacco DDoS, ripristinando la piena operatività. È fondamentale considerare sia gli impatti numerici ovvero quantitativi che quelli qualitativi per per affrontare efficacemente i rischi e garantire la resilienza dell'organizzazione.

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.

Misure di risposta per contenere l’infezione (malware)

Quando l'applicazione web viene infettata da un malware, la nostra priorità è impedire che il malware si propaghi all'interno della rete. In questo contesto, non siamo interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Vogliamo piuttosto contenere l'infezione e proteggere il resto dell'infrastruttura. Ecco alcune risposte:

Isolamento della macchina compromessa

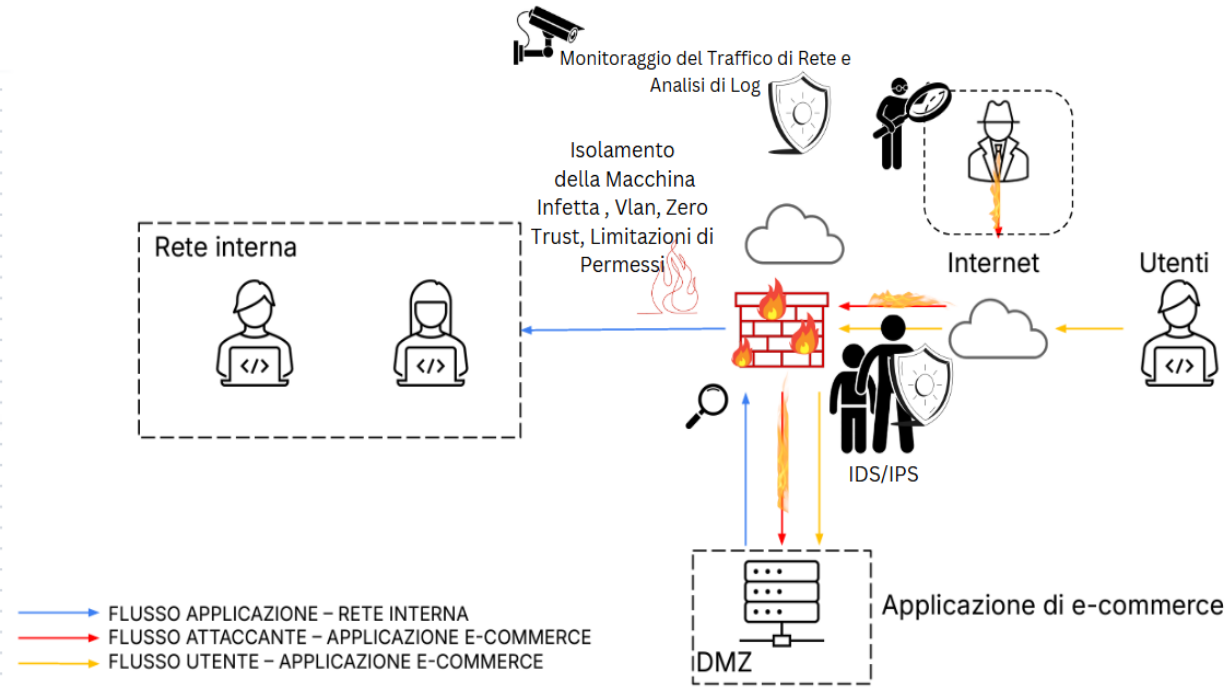
Il primo passo è isolare immediatamente la macchina compromessa per impedire al malware di diffondersi ad altri sistemi. Possiamo farlo disconnettendo la macchina dalla rete principale e spostandola in una VLAN isolata o una subnet separata. Utilizzando tecniche di segmentazione della rete e adottando un'architettura Zero Trust, isoliamo completamente il server compromesso e limitiamo rigorosamente le sue comunicazioni con il resto dell'infrastruttura. Questo isolamento impedisce al malware di propagarsi, proteggendo gli altri dispositivi della rete. In questa fase puo essere utile anche limitare i permessi e controllare gli accessi sulla macchina compromessa impedendo al malware di eseguire azioni dannose che richiedono autorizzazioni elevate. In sinergia con l'architettura Zero Trust, offre livelli multipli di sicurezza: se una misura fallisce, l'altra fornisce protezione aggiuntiva.

Monitoraggio del traffico di rete

Implementare sistemi di monitoraggio del traffico è essenziale per identificare attività anomale provenienti dalla macchina compromessa. Analizzando i log di rete, possiamo rilevare tentativi di comunicazione del malware con server esterni o con altri dispositivi interni. Questo ci permette di intervenire tempestivamente per bloccare eventuali canali di propagazione o esfiltrazione di dati.

Firewall e IDS/IPS

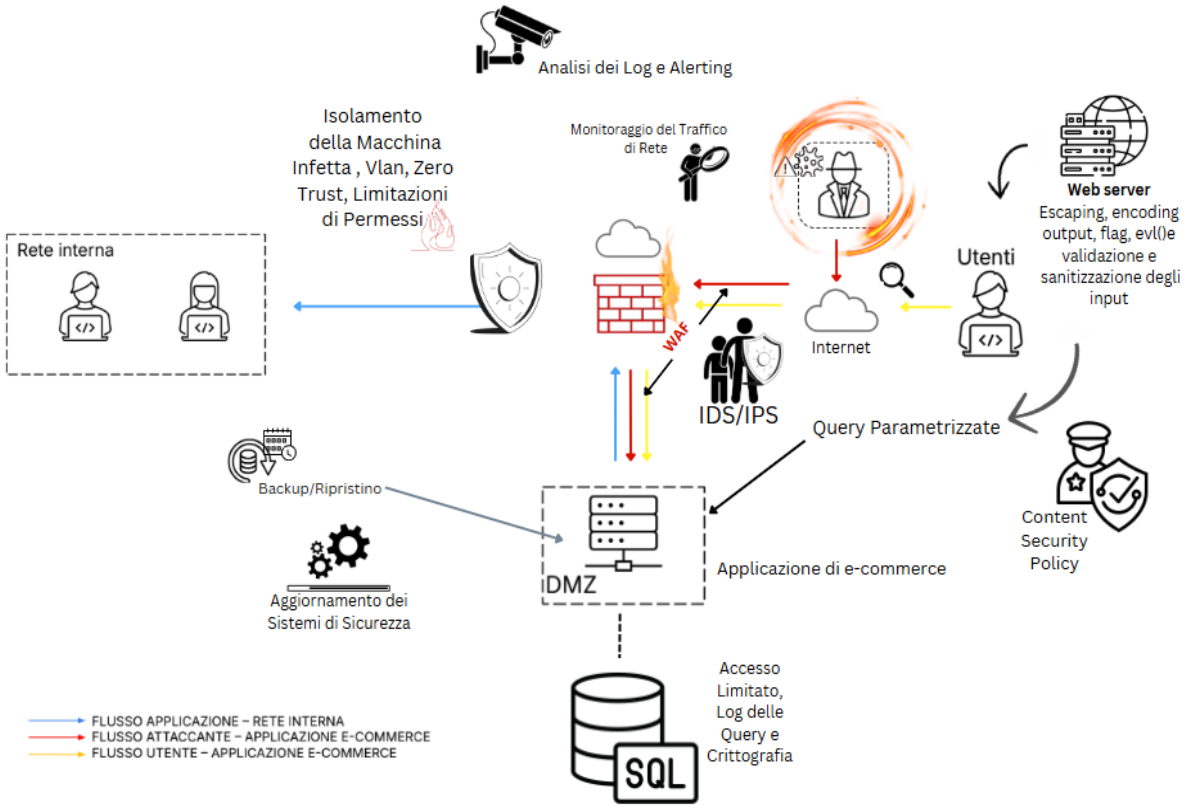
Configurare i firewall per bloccare il traffico in uscita dalla macchina compromessa verso destinazioni sconosciute o sospette è un passo fondamentale. L'utilizzo di sistemi di Intrusion Detection e Intrusion Prevention (IDS/IPS) aiutano a individuare e fermare tentativi di diffusione del malware. Questi sistemi possono rilevare comportamenti anomali o pattern noti di attacchi, permettendoci di agire rapidamente per contenere l'infezione.



Una volta che un incidente di sicurezza viene rilevato, le misure di risposta entrano in gioco per gestire l'incidente.Poiché non rimuoviamo l'accesso dell'attaccante alla macchina infetta, possiamo monitorare le sue attività per raccogliere informazioni utili. Successivamente, è importante condurre un'analisi forense per determinare l'origine e l'impatto dell'infezione. Questo ci aiuta a comprendere meglio le tecniche e gli obiettivi dell'attaccante, facilitando la prevenzione di futuri attacchi.

Ricordiamo inoltre che è buona prassi fare backup regolari e aggiornare costantemente i sistemi di sicurezza. Questo assicura la possibilità di ripristinare l'operatività rapidamente in caso di incidenti e riduce le vulnerabilità sfruttabili dagli attaccanti.

4. Soluzione completa: unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)



Unire misure preventive per proteggere l'applicazione web da attacchi SQLi e XSS accompagnandole con interventi di risposta rapidi per contenere la diffusione del malware nella rete, è fondamentale per garantire una sicurezza completa. Implementando soluzioni come il Web Application Firewall (WAF), la parametrizzazione delle query, la validazione e sanitizzazione degli input e la CSP, possiamo ridurre significativamente i rischi legati a vulnerabilità comuni. Inoltre, la protezione dei cookie tramite i flag HTTPOnly e Secure, insieme al monitoraggio continuo delle attività sospette, contribuisce a mantenere elevati standard di sicurezza. Questo approccio integrato offre una difesa attiva, capace di reagire tempestivamente a un attacco, isolando le macchine compromesse e limitando la propagazione del malware. In questo modo, si garantisce non solo la protezione dei dati sensibili, ma anche la continuità operativa dell'applicazione.

5. Modifica «più aggressiva» dell'infrastruttura (se necessario/facoltativo magari integrando la soluzione al punto 2)

Per rafforzare la sicurezza, possiamo adottare tecnologie avanzate e azioni mirate. L’introduzione di un sistema automatizzato che identifica e risponde alle minacce in tempo reale, utilizzando intelligenza artificiale e machine learning, ci permetterà di rilevare rapidamente anomalie e attacchi. Inoltre, automatizzare l'aggiornamento delle patch assicura che i sistemi siano sempre protetti contro le vulnerabilità più recenti.
Implementando soluzioni SIEM per monitorare l'intera infrastruttura e integrando fonti di threat intelligence, resteremo sempre proattivi nei confronti di nuove minacce. Il sandboxing ci consentirà di isolare e analizzare applicazioni sospette senza compromettere il sistema principale. Inoltre, test di penetrazione regolari e simulazioni di attacchi, condotte da un red team, ci aiuteranno a rafforzare ulteriormente le difese.
La gestione degli accessi sarà rigorosa grazie agli strumenti IAM, limitando l'accesso alle informazioni sensibili solo agli utenti autorizzati. Infine, automatizzeremo le risposte agli incidenti con playbook dettagliati, riducendo i tempi di reazione e contenendo gli impatti.
Con queste azioni, costruiremo una difesa multilivello che renderà il nostro sistema più robusto e “aggressivo” nella protezione. Miglioreremo la capacità di rilevare, prevenire e rispondere rapidamente alle minacce, garantendo la sicurezza dell’infrastruttura e la continuità operativa, sempre un passo avanti rispetto agli attaccanti.