EPICODE

Progetto S9 – L5

TRACCIA

Con riferimento alla figura sotto, 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 (una sola modifica).

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 vostra rete, mentre non siete interessati a rimuovere l’accesso da parte dell’attaccante alla macchina infettata. Modificate la figura 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: integrando eventuali altri elementi di sicurezza (se necessario/facoltativo magari integrando la soluzione al punto 2).

Immagine che contiene testo, diagramma, schermata, Carattere

Descrizione generata automaticamente

SOLUZIONE

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 (una sola modifica).

- Un’ottima soluzione per prevenire attacchi come XSS e SQLi da parte di un attaccante è quella di sanificare il codice garantendo che i dati input siano opportunamente filtrati.  
Questa pratica, tuttavia, prevede la revisione dell’intero codice e richiede dunque un importante investimento in termini economici e di tempo.  
Come soluzione alternativa si è quindi scelto di implementare un WAF (Web Application Firewall) che è in grado di rilevare e bloccare attacchi XSS e SQLi. Nella figura sotto è possibile vedere l’aggiunta del WAF.

Immagine che contiene testo, schermata, diagramma, Carattere

Descrizione generata automaticamente

segue

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.

- L’impatto sul business subito può essere calcolato moltiplicando la spesa media al minuto da parte degli utenti per il numero di minuti in cui l’applicazione è rimasta non raggiungibile.  
1.500 € x 10 = 15.000 € (danno subito da un punto di vista quantitativo).  
Da un punto di vista qualitativo è probabile che l’interruzione possa generare una perdita di fiducia da parte dei clienti. Probabilmente il danno subito, tenendo conto di un lasso di tempo più lungo dell’immediato, è quindi superiore ai 15.000 € precedentemente calcolati.

Per ridurre la probabilità di subire una nuova interruzione del servizio a causa di un DDos è possibile eseguire alcune azioni preventive. Tra cui:

Monitoraggio: Implementare un sistema di monitoraggio per rilevare anomalie, come picchi di traffico sospetti o comportamenti insoliti. Importante per accorgersi in tempo dell’attacco.

Bilanciamento del carico: Distribuire il carico su più server o servizi per ridurre l’impatto di un attacco su un singolo punto di accesso.

Cloud-based DDoS protection services: Sottoscrivere servizi di protezione DDoS offerti da fornitori cloud o terze parti. Questi servizi possono rilevare e mitigare automaticamente gli attacchi DDoS, spostando il traffico malevolo lontano dal tuo server.

Backup e failover: Avere un piano di backup e procedure di failover per garantire la continuità del servizio in caso di attacco.

Come è possibile notare nell’immagine sotto si è optato per un failover cluster.

Immagine che contiene testo, diagramma, schermata, linea

Descrizione generata automaticamente

3. Response: l’applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostra rete, mentre non siete interessati a rimuovere l’accesso da parte dell’attaccante alla macchina infettata. Modificate la figura con la soluzione proposta.

- Per evitare che il malware si propaghi nella rete interna può essere applicata la tecnica dell’isolamento. Questa tecnica disconnette completamente l’applicazione web dalla rete. In questo modo l’attaccante ha ancora accesso alla macchina ma non può più spostarsi nella rete essendone fuori. Questa situazione può essere utile per studiarne il comportamento senza eccessivi rischi. L’immagine sotto mostra la situazione.

Immagine che contiene testo, diagramma, schermata, Piano

Descrizione generata automaticamente

segue

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

- Si riporta nell’immagine sotto la soluzione completa di prevenzione agli attacchi XSS e SQLi e di response.

Immagine che contiene testo, diagramma, schermata, Carattere

Descrizione generata automaticamente

Segue

5. Modifica <più aggressiva> dell’infrastruttura: integrando eventuali altri elementi di sicurezza (se necessario/facoltativo magari integrando la soluzione al punto 2).

- La modifica <più aggressiva> dell’infrastruttura prevede diversi interventi, tra cui:

L’implementazione di un WAF (Web Application Firewall) che è in grado di rilevare e bloccare attacchi XSS e SQLi.

L’implementazione di un failover cluster sulle applicazioni web per resistere meglio agli attacchi DDos, per poter effettuare bilanciamento del carico e per garantire la continuità del servizio anche in caso di problemi su una delle due applicazioni.

L’aggiunta di un IPS (Intrusion Prevention System) a difesa della rete interna. L’IPS, che è sempre aggiornato sui possibili pericoli, è infatti in grado di rilevare potenziali minacce e bloccarle prima che possano raggiungere la rete interna.

Immagine che contiene testo, schermata, diagramma, Carattere

Descrizione generata automaticamente

BONUS

TRACCIA

Analizzare le seguenti segnalazioni caricate su anyrun e fare un piccolo report di ciò che si scopre relativo alla segnalazione dell’eventuale attacco spiegando ad utenti e dirigenti la tipologia di attacco e come evitare questi attacchi in futuro:  
1. https://app.any.run/tasks/8e6ad6d9-4d54-48e8-ad95-bfb67d47f1d7/  
2. https://app.any.run/tasks/60b9570f-175b-4b03-816b-a38cc2b0255e/

SOLUZIONE

1. <https://app.any.run/tasks/8e6ad6d9-4d54-48e8-ad95-bfb67d47f1d7/>

Modifiche ai criteri di esecuzione di PowerShell (senza restrizioni): Il malware potrebbe aver alterato le impostazioni di sicurezza di PowerShell, consentendo l’esecuzione di comandi dannosi senza restrizioni. Questo potrebbe essere utilizzato per scopi malevoli.

Elimina il file eseguibile immediatamente dopo l’avvio: Il malware sembra eliminare sé stesso subito dopo essere stato avviato. Questo è un tentativo di nascondere la sua presenza e rendere difficile la sua rilevazione.

In breve, questo malware potrebbe compromettere la sicurezza del sistema ed eseguire comandi dannosi. È importante rimuoverlo immediatamente.

Si esegue su Windows 7, è necessario passare ad un sistema operativo più recente come Windows 11.

2. <https://app.any.run/tasks/60b9570f-175b-4b03-816b-a38cc2b0255e/>

Elimina file eseguibili: Il malware cancella immediatamente i file eseguibili (programmi) dopo l’avvio.

Processi sospetti: Alcuni processi (come iexplore.exe, MicrosoftEdgeSetup.exe, ecc.) eliminano file legittimi di Windows.

Contenuto sovrascritto: Il malware modifica o cancella il contenuto di file eseguibili.

Avvio da posizioni insolite: Si avvia da percorsi non comuni.

Disabilita SEHOP: Disattiva una protezione di sicurezza di Windows.

Crea/modifica pianificazione attività COM: Modifica le attività pianificate di Windows.

Voce di disinstallazione del software: Crea una voce di disinstallazione falsa.

Legge impostazioni Internet e certificati di sistema: Raccoglie informazioni sensibili.

Controlla attendibilità di Windows: Verifica le impostazioni di sicurezza.

Esecuzione come servizio Windows: Si nasconde come servizio di sistema.

Legge impostazioni di sicurezza di Internet Explorer: Analizza le impostazioni del browser.

In breve, questo malware è molto pericoloso e dovrebbe essere rimosso immediatamente.

Anche questo malware si esegue su Windows 7. Passare ad un sistema operativo più recente è la soluzione.