BENCHMARK W20D4 - Domenico Vecchio

TRACCIA:

Con riferimento alla figura in slide 2, rispondere ai seguenti quesiti.
1. **Azioni preventive:** quali azioni preventive si potrebbero implementare per difendere l'applicazione Wep App attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato. Modificate la figura in modo da evidenziare le implementazioni.

1. **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 diazioni preventive che si possono applicare in questa problematica.

1.**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 rimuovere l'accesso da parte dell'attaccante alla macchina infettata.
Modificate la figura in slide 2 con la soluzione proposta.

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

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

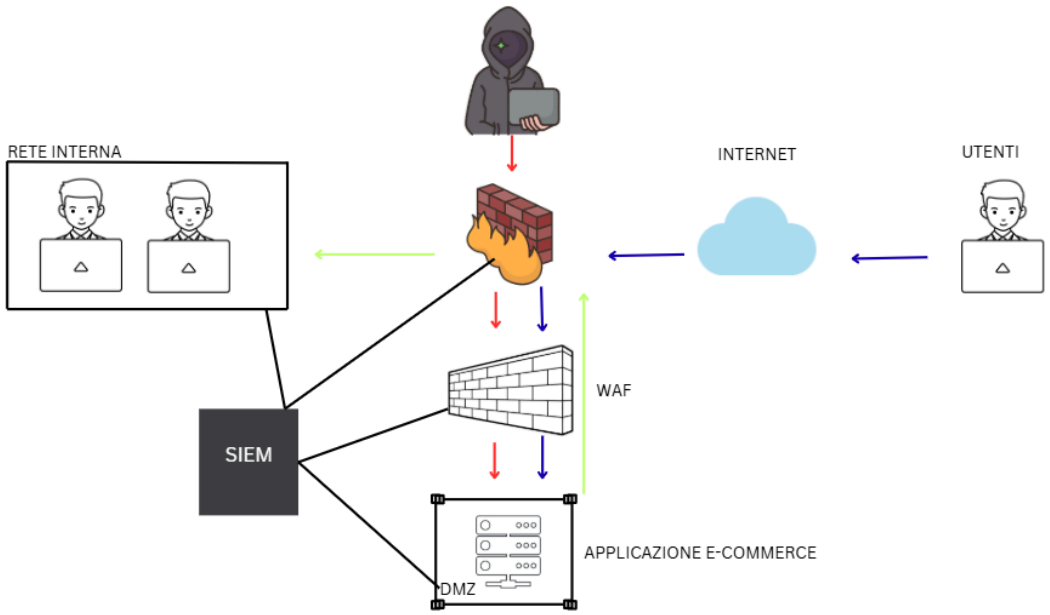
SOLUZIONE :

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

Per la protezione della Web App da minacce XSS e SQLi si può utilizzare una soluzione basata su Web Application Firewall , dedicato a proteggere le Web App da attacchi . La soluzione prevede l'inserimento di un SIEM che riceva informazioni di input della rete interna . firewall , WAF e DMZ .

Architettura :
Garantire che l'applicazione e-commerce sia accessibile agli utenti da Internet, ma con una rete interna protetta da eventuali compromissioni.

Grafico :



Componenti principali

1. **Utenti (Internet)**

   Gli utenti accedono all'applicazione tramite Internet.

2. **Applicazione di e-commerce (nella DMZ)**

   Il server dell'applicazione si trova nella DMZ (Demilitarized Zone), una zona di rete intermedia accessibile da Internet ma isolata dalla rete interna per sicurezza.

3. **Firewall/WAF (Web Application Firewall)**

   Protegge l'applicazione filtrando il traffico in entrata. Può bloccare traffico malevolo come SQL injection, XSS.

4. **SIEM**

   Sistemi di monitoraggio e risposta agli eventi di sicurezza. Raccolgono e analizzano i log, automatizzano risposte a minacce e inviano alert.

5. **Rete interna**

   Dove si trovano sistemi aziendali critici. Accesso molto limitato e sorvegliato.

Flussi di traffico (colorati)

- **Flusso applicazione** → rete interna

  Comunicazione tra l'app e i sistemi interni (es. database, servizi interni). Va regolata bene, perché se un attaccante compromette il server e-commerce, potrebbe tentare di accedere alla rete interna.

- **Flusso attaccante** → applicazione e-commerce

  Simula un attacco proveniente da Internet. Questo flusso è monitorato e filtrato dal WAF e dal SIEM/SOAR.

- **Flusso utente** → applicazione e-commerce

  Rappresenta l'uso legittimo da parte degli utenti finali che navigano e acquistano sulla piattaforma.

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.

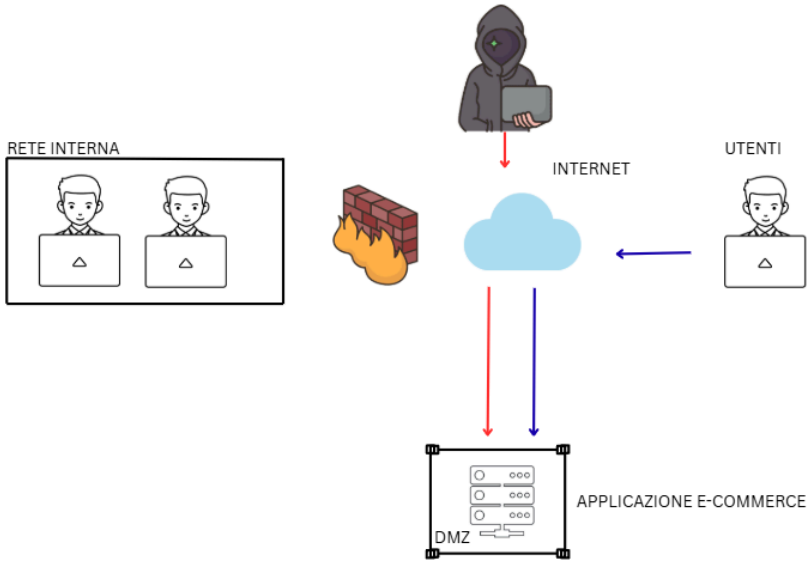
L'attacco di tipo Ddos causa la non raggiungibilità della piattaforma di e-commerce per 10 minuti.
Considerando che gli utenti spendono circa 1.500€ al minuto, possiamo stimare i danni causati dal mancato guadagno sul business moltiplicando la spesa potenziale degli utenti per minuto (1.500€) per i minuti di indisponibilità del servizio (10).
Impatto sul business = 1.500 € x 10 minuti = 15.000 €
Ovvero per 10 minuti di indisponibilità la compagnia ha perso 15.000 € di acquisti potenziali.

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 rimuovere l'accesso da parte dell'attaccante alla macchina infettata.

Considerata la priorità, si può adottare una strategia basata sull'isolamento della macchina infettata. In questo caso la macchina sarà direttamente collegata ad internet, raggiungibile dall'attaccante ma non più connessa alla rete interna.

Quando si scopre che un server (come quello dell'applicazione e-commerce) è stato compromesso, la priorità è impedire che l'attaccante possa muoversi lateralmente verso la rete interna.

Grafico :



Descrizione del grafico

Rispetto al grafico precedente, ci sono modifiche chiave:

Presenza:

1. Utente esterno (Internet)
   Può ancora accedere all'applicazione web e-commerce.

2. Attaccante
   Ha ancora visibilità e accesso alla macchina e-commerce perché è pubblica (in DMZ).

3. Applicazione di e-commerce
   Ancora disponibile su Internet, ma isolata.

Assenza:

- **Rete interna:**

  Non comunica più con la macchina compromessa (nessuna freccia blu).
  In pratica, è stato rimosso il flusso di rete tra la DMZ e la rete interna per evitare escalation.

- **SIEM:**

  Sparito dal diagramma, perché l'obiettivo qui è la separazione netta e urgente.

Flussi evidenziati:

- **Flusso utente** → applicazione e-commerce: ancora attivo.
- **Flusso attaccante** → applicazione e-commerce: ancora presente.
- **Flusso applicazione** → rete interna: non più presente (rimosso come contromisura).

Obiettivo di questa strategia

Limitare il danno:

- L'attaccante non può più raggiungere risorse sensibili o critiche della rete interna.
- Il server infetto resta isolato (può essere monitorato o spento successivamente).

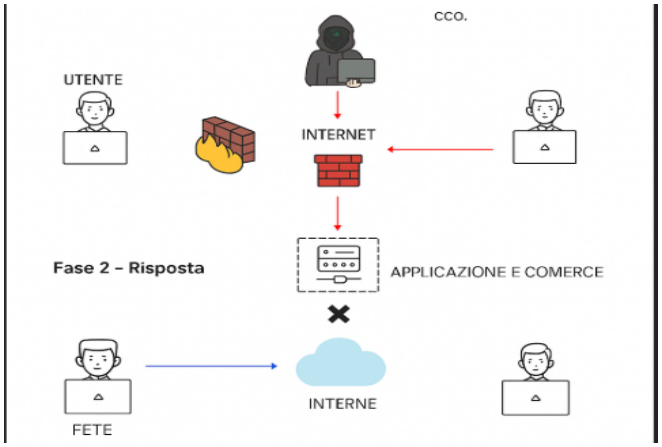
Considerazioni tecniche:

- Questo tipo di isolamento può essere fatto modificando le regole del firewall o tramite un sistema di segmentazione dinamica.
- È una strategia reattiva ma efficace in caso di compromissione.

Il diagramma evidenzia che la rete interna è raggiungibile dalla DMZ in base alle policy del firewall. Se il server in DMZ viene compromesso, un attaccante potrebbe tentare di penetrare nella rete interna: per questo motivo, è fondamentale configurare con attenzione il firewall e monitorare tutto con sistemi SIEM.

3. **Soluzione completa :** Unione dei due grafici del punto 1 e 3

Grafico :



Spiegazione dello schema

Lo schema rappresenta una soluzione completa di sicurezza per un'applicazione di e-commerce esposta su Internet**.**

Si articola in due fasi:

Fase 1 – Prevenzione

Questa è l'architettura iniziale della rete, progettata per garantire sicurezza e disponibilità del servizio:

- Gli utenti accedono all'applicazione tramite Internet.
- Un WAF (Web Application Firewall) filtra le richieste e protegge da attacchi noti.
- Il traffico viene monitorato da un SIEM/SOAR, che registra eventi e anomalie.
- -L'applicazione è in DMZ, isolata parzialmente dalla rete interna ma comunque autorizzata a comunicare con essa.

Fase 2 – Risposta

In caso di compromissione dell'applicazione:

- Viene interrotta ogni connessione tra la DMZ e la rete interna, per evitare l'espansione dell'attacco.
- Il server compromesso resta raggiungibile da Internet (es. per raccolta forense), ma viene isolato da tutte le risorse aziendali interne.
- Continuano le attività di monitoraggio, e possono essere attivate risposte automatiche.

Conclusione

Unire prevenzione e risposta è essenziale per costruire una difesa a strati (defense-in-depth).

La prevenzione riduce il rischio di compromissione, mentre la risposta tempestiva limita i danni e protegge le risorse critiche.

Questa strategia consente all'azienda di mantenere l'operatività anche in presenza di minacce, garantendo sicurezza, resilienza e capacità di reazione.