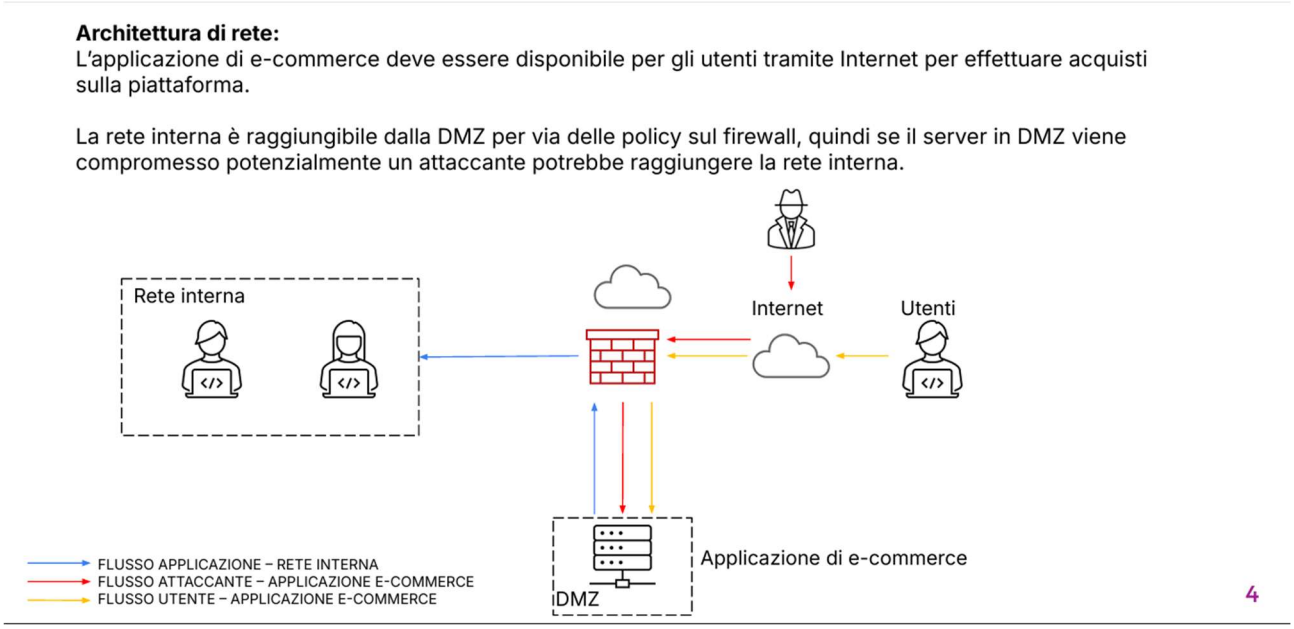
Consegna w20d4

TRACCIA:Con riferimento alla figura suguente, 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 vostra rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura con la soluzione proposta.



1. Azioni Preventive: Difesa contro SQL Injection (SQLi) e Cross-Site Scripting (XSS)

1.1. Spiegazione delle minacce

SQL Injection (SQLi) e **Cross-Site Scripting (XSS)** sono tra le vulnerabilità più sfruttate dagli attaccanti per compromettere la sicurezza delle applicazioni web. Gli attacchi SQLi mirano a manipolare le query SQL inviate al database tramite input non validati, consentendo l'accesso, la modifica o la cancellazione di dati sensibili. Gli attacchi XSS, invece, permettono l'iniezione di script malevoli nelle pagine web, con l'obiettivo di rubare sessioni utente, diffondere malware o manipolare i contenuti visualizzati.
Le conseguenze di questi attacchi possono essere devastanti e molteplici come la perdita di dati e l'interruzione dei servizi.

1.2. Misure preventive

1.Validazione e sanificazione degli input
La validazione degli input consiste nel controllare che i dati inseriti dagli utenti rispettino il formato atteso (es. numeri, email, URL), mentre la sanificazione rimuove o neutralizza caratteri potenzialmente pericolosi.

Queste pratiche sono fondamentali per prevenire sia SQLi che XSS.

2. Segmentazione e Micro-segmentazione

La segmentazione della rete e la micro-segmentazione limitano i movimenti laterali di un attaccante che dovesse compromettere un componente della DMZ (rete perimetrale che ospita i servizi pubblici e protegge la LAN interna, un livello di sicurezza tra Internet e l'azienda) isolando i servizi e riducendo la superficie di attacco.

3. Gestione delle Patch e Vulnerabilità

L'aggiornamento tempestivo dei sistemi operativi, framework e librerie è di cruciale importanza per chiudere l'accesso ai sistemi tramite l'utilizzo di vulnerabilità note

4. Controllo degli accessi e IAM

L'utilizzo di sistemi di Identity and Access Managment (IAM) insieme all'utilizzo del concetto di minimo privilegio (ovvero ogni utente e processo deve avere solo i permessi strettamente necessari per svolgere il proprio compito) riduce l'area di attacco in quanto si previene che un attaccante possa sfruttare molteplici credenziali compromesse

5. Web Application Firewall (WAF)

Un WAF analizza il traffico HTTP/HTTPS in ingresso, bloccando automaticamente richieste sospette che contengono pattern riconducibili a SQLi, XSS o altre vulnerabilità. Il WAF può essere implementato nella DMZ, davanti al server web, per una protezione multilivello.

2. Impatti sul Business: Attacco DDoS e Calcolo dell'Impatto Economico

2.1 Spiegazione dell'attacco DDoS e calcolo della perdita stimata

Un attacco Distributed Denial of Service (DDoS) mira a saturare le risorse di rete, di calcolo o di memoria di un servizio, rendendolo inaccessibile agli utenti. Nel caso in esame, l'applicazione e-commerce subisce un attacco che la rende indisponibile per 10 minuti.

Sapendo che il profitto commerciale per minuto è di 1.500€ e la durata di downtime è di 10 minuti ci basta moltiplicare il profitto per la durata e avremo come risultato l'impatto economico.

TOTALE PERDITA STIMATA: 1.500 € * 10 = 15.000 €

2.2 Strategie di Mitigazione e Interventi

Soluzioni On-Premise

Firewall avanzati con protezione DDoS: filtraggio del traffico in ingresso e blocco di IP sospetti.

IDS/IPS: rilevamento di pattern di attacco e blocco automatico.

Segmentazione della rete: isolare i servizi critici per limitare l'impatto di eventuali attacchi.

Soluzioni Cloud e Ibride

DDoS Protection as a Service: uso di servizi esterni (ad esempio Cloudflare, AWS Shield) che bloccano e/o mitigano automaticamente gli attacchi lasciando in questo modo il sito online

CDN e Load Balancer: distribuire su più server i contenuti in modo che il sito riesce a reggere meglio il traffico

Failover e ridondanza geografica: replica dei servizi su più data center per garantire la continuità operativa.

Best Practice Organizzative

Piani di risposta agli incidenti: definizione di ruoli, procedure e canali di comunicazione.

Test periodici di resilienza: simulazioni di attacco per valutare la capacità di risposta.

3. Response: Gestione di un'Infezione Malware sull'Applicazione Web

3.1. Scenario: Infezione Malware

L'applicazione web viene infettata da un malware, con potenziale rischio di propagazione nella DMZ e verso la rete interna. Diventa dunque di fondamentale importanza attivare un piano di Incident Response strutturato.

3.2. Azioni Immediati (nelle prime ore)

- Identificazione e Triage

La fase di identificazione e triage è un momento di filtro e contenimento: si passa dal rilevamento dell'anomalia alla valutazione della sua gravità, fino all'isolamento del sistema compromesso. Un approccio strutturato, basato su strumenti di monitoraggio e procedure standard, consente di reagire in modo rapido ed efficace, minimizzando l'impatto dell'incidente.

- Contenimento

La fase di contenimento combina misure tecniche (segmentazione e firewall) con procedure forensi (preservazione delle evidenze). In questo modo si ottiene un duplice vantaggio quello di bloccare la propagazione dell'attacco e proteggere la rete interna sia quello di garantire materiale di analisi per comprendere l'origine, la natura e l'impatto dell'incidente.

- Comunicazione

La comunicazione durante un incidente deve essere rapida, strutturata e controllata. Notificare subito il team IR e i responsabili IT, informare il personale con procedure chiare e impedire la diffusione incontrollata di informazioni sono elementi chiave per una gestione efficace della crisi.

3.3. Azioni nelle 24 Ore

- Analisi e Investigazione

Dopo aver contenuto l'incidente, è fondamentale avviare una fase di analisi e investigazione per capire davvero cosa è successo. Si parte dai log di sistema, applicazione e rete, che permettono di ricostruire il vettore di attacco e la portata dell'infezione. Parallelamente, il malware viene eseguito in un ambiente sandbox isolato, così da osservare il suo comportamento senza rischi: in questo modo si possono estrarre indicatori di compromissione e aggiornare le difese.
Un altro passo cruciale è la verifica dei backup: bisogna controllarne l'integrità e assicurarsi che non siano stati contaminati, così da avere copie sicure per il ripristino. Questa fase non serve solo a risolvere l'incidente, ma anche a raccogliere informazioni preziose per migliorare le procedure di sicurezza e prevenire futuri attacchi.

- Eradicazione

La fase di eradicazione rappresenta il momento in cui l'organizzazione passa dal contenimento alla vera e propria eliminazione della minaccia. Il primo passo consiste nella rimozione del malware. Nei casi più gravi, quando il sistema risulta compromesso in profondità, la scelta migliore è la reinstallazione da immagini pulite (golden image), che assicura un ambiente totalmente privo di residui malevoli. Successivamente, è indispensabile procedere con l'applicazione di patch e aggiornamenti. Ogni vulnerabilità sfruttata deve essere chiusa immediatamente, portando il sistema e le applicazioni alla versione più sicura e stabile. Infine, si interviene sulla componente identitaria: reset delle credenziali e invalidazione dei token di sessione. Questo passaggio è fondamentale per impedire che un attaccante possa continuare ad accedere con account compromessi o sessioni ancora attive.

- Ripristino e Recovery

La fase di ripristino e recovery segna il momento in cui l'organizzazione riporta i sistemi compromessi a uno stato operativo sicuro. Dopo l'eradicazione del malware, è necessario ricostruire l'ambiente partendo da

backup verificati. Una volta ripristinati i sistemi, si procede con un monitoraggio rafforzato: controlli continui su processi, traffico di rete e log per individuare eventuali persistenze del malware o tentativi di reinfezione. In questa fase si applicano regole di sicurezza più stringenti e si utilizzano strumenti di detection avanzata per validare la stabilità dell'ambiente. Infine, prima di riaprire i servizi agli utenti, è indispensabile eseguire test di funzionalità e sicurezza. Questi test verificano che le applicazioni rispondano correttamente, che i dati siano integri e che le misure di protezione siano attive.

- Comunicazione e Reporting
La comunicazione e il reporting non sono attività accessorie, ma parte integrante della gestione dell'incidente. Aggiornare le parti interessate e documentare in modo rigoroso ogni evidenza consente di mantenere fiducia, rispettare gli obblighi normativi e trasformare l'incidente in un'occasione di miglioramento continuo.

3.4. Best Practice e Considerazioni Didattiche
La gestione degli incontri di sicurezza richiede una preparazione accurata. Prima che un incidente si verifichi è fondamentale stabilire responsabilità precise e linee di comunicazione interne, in modo che ogni membro del team sappia cosa fare e a chi riportare le informazioni. Questa fase di preparazione riduce i tempi di reazione e a limitare gli errori. Un altro elemento chiave sono le simulazioni periodiche che consentono di testare la prontezza del team e verificare l'efficacia delle procedure. Durante la gestione dell'incidente è importante anche garantire la preservazione delle prove. Log, immagini di memoria e copie disco devono essere raccolti e conservati secondo metodologie forensi, così da mantenere la loro validità in eventuali indagini legali. Infine il piano di Incident Response deve essere considerato un documento dinamico, quindi come un documento da aggiornare continuamente sulla base delle lezioni apprese e dell'evoluzione delle minacce.

Conclusioni e Raccomandazioni

L'esercizio proposto offre una panoramica completa delle strategie di sicurezza per un'applicazione e-commerce in DMZ, integrando misure preventive, di detection e di risposta. La chiave per una postura di sicurezza efficace è la combinazione di controlli tecnici, organizzativi e formativi, supportati da una governance solida e da una cultura della sicurezza diffusa.