REPORT PROGETTO S9/L5

22/03/2024

Prepared By:
Ayman Hani

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 Web da attacchi di tipo SQLioppure 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 DDoSdall'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

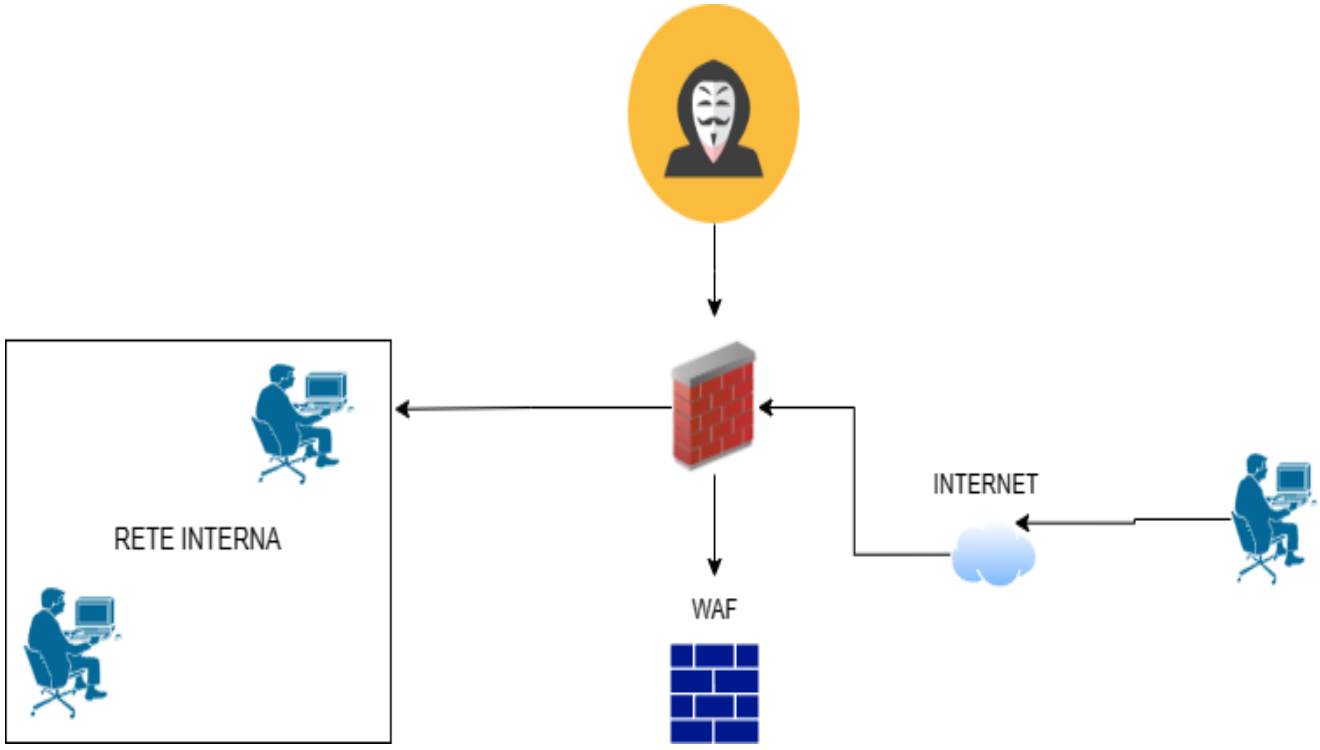
3.Response: l'applicazione Web viene infettata da un malware. La vostra priorità è che il malwarenon si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura in slide 2 con la soluzione proposta .

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

INDICE

AZIONI PREVENTIVE

Come azione preventiva per proteggere la web app da attacchi xss e SQL injection è saggio utilizzare un Web Application Firewall dato che sono progettati apposta per quel tipo di attacco. La figura va modificata aggiungendo semplicemente un WAF tra la DMZ e il firewall



IMPATTI SUL BUSINESS

L'attacco DDoS ha causato un interruzione del servizio per 10 minuti. Durante questo lasso di tempo, i clienti non sono stati in grado di accedere al sito e hanno di conseguenza speso i loro soldi su altre piattaforme di e-commerce.

La perdita economica stimata per l'azienda a seguito dell'attacco è di 15.000 €. Questa cifra è stata calcolata basandosi sulla spesa media dei clienti di 1.500 € al minuto su piattaforme alternative durante il periodo di inattività.

L'attacco DDoS ha evidenziato la vulnerabilità dell'applicazione web di e-commerce e l'importanza di implementare misure di sicurezza robuste per prevenire o mitigare gli effetti di tali attacchi.

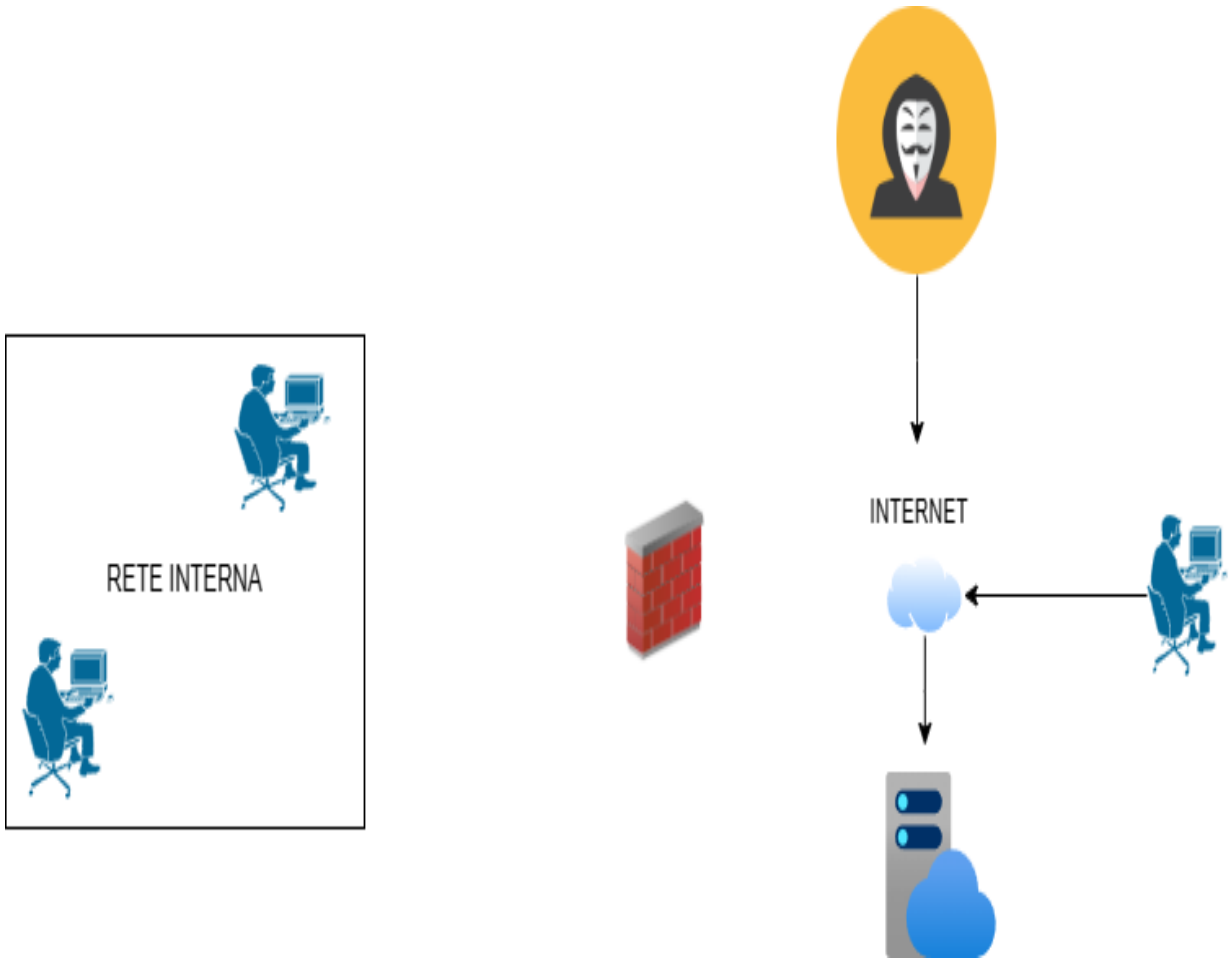
La perdita economica subita sottolinea la necessità di una strategia di risposta rapida e efficace in caso di incidenti di sicurezza informatica.

RESPONSE

Dato che vogliamo evitare che il malware si diffonda ma allo stesso tempo la nostra priorità non riguarda vietare l'accesso alla macchina infettata da parte dell' hacker procederemo con la strategia dell'isolamento, facendo ciò la macchinma resterà collegata a internet ma non alla rete interna.

SOLUZIONE COMPLETA

Isoliamo la macchina infetta



BONUS

L’allarme generato dall’applicazione ANY.RUN indica il rilevamento di un potenziale attacco informatico. La segnalazione specifica il sospetto malware denominato “PERFORMANCE.BOOSTER.3.8.exeIl tipo di attacco sembra coinvolgere un software dannoso (malware) che potrebbe essere stato scaricato involontariamente sul sistema.

Questo malware potrebbe danneggiare il computer o compromettere la sicurezza dei dati. Per evitare attacchi simili in futuro, si consiglia di: Formazione dei Dipendenti: Assicurarsi che tutti i dipendenti siano in grado di riconoscere potenziali email di phishing o download dannosi.

Aggiornamenti Regolari: Mantenere aggiornati tutti i software e i sistemi operativi per correggere eventuali vulnerabilità note.Installazione di Software

Antivirus: Utilizzare software antivirus affidabili per rilevare e mitigare le minacce.Evitare Download

Sospetti: Evitare di scaricare file o cliccare su link provenienti da fonti non affidabili.

Utilizzo di Firewall: Attivare i firewall per bloccare l’accesso non autorizzato alla rete.

È fondamentale rimanere vigili e informati sulle minacce emergenti e implementare misure preventive in modo proattivo per migliorare la postura di cybersecurity all’interno dell’organizzazione.