M5-W20D4: Progetto fine modulo

DATA

Cybersecurity Analyst

Studente:
Andrea Scarmagnani
Docente:
Federico Daidone

Cyber Security & Ethical Hacking Giorno 5 – Progetto

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 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

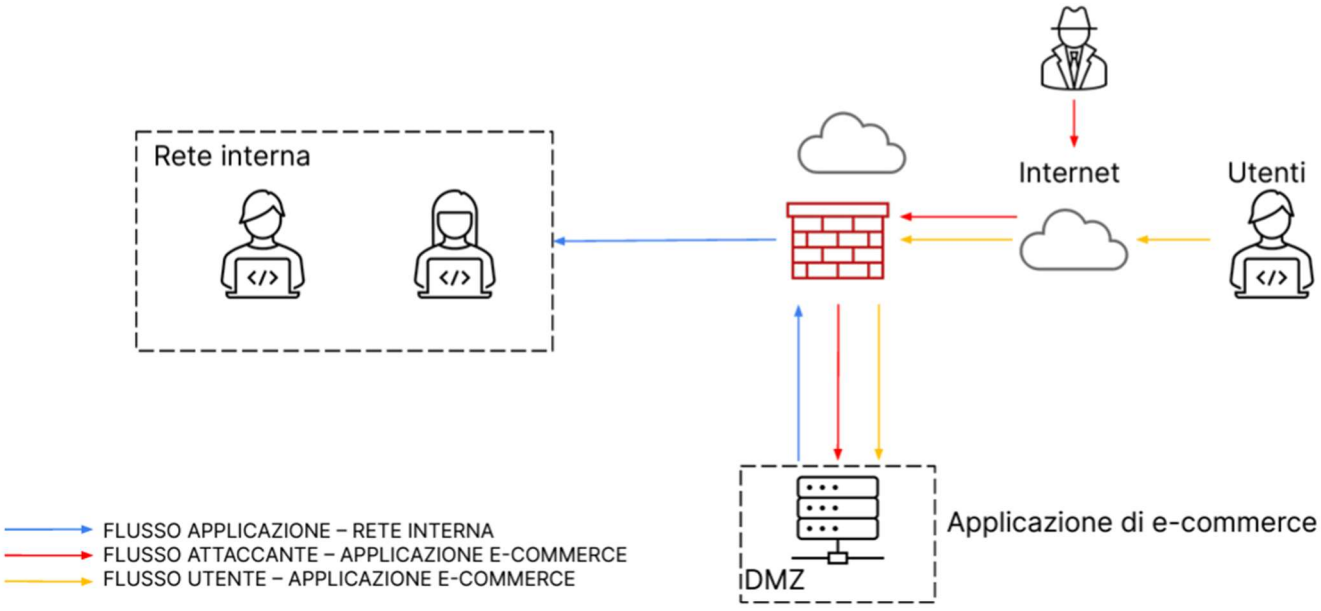
3. Response: l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura in slide 2 con la soluzione proposta.

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

5. 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.

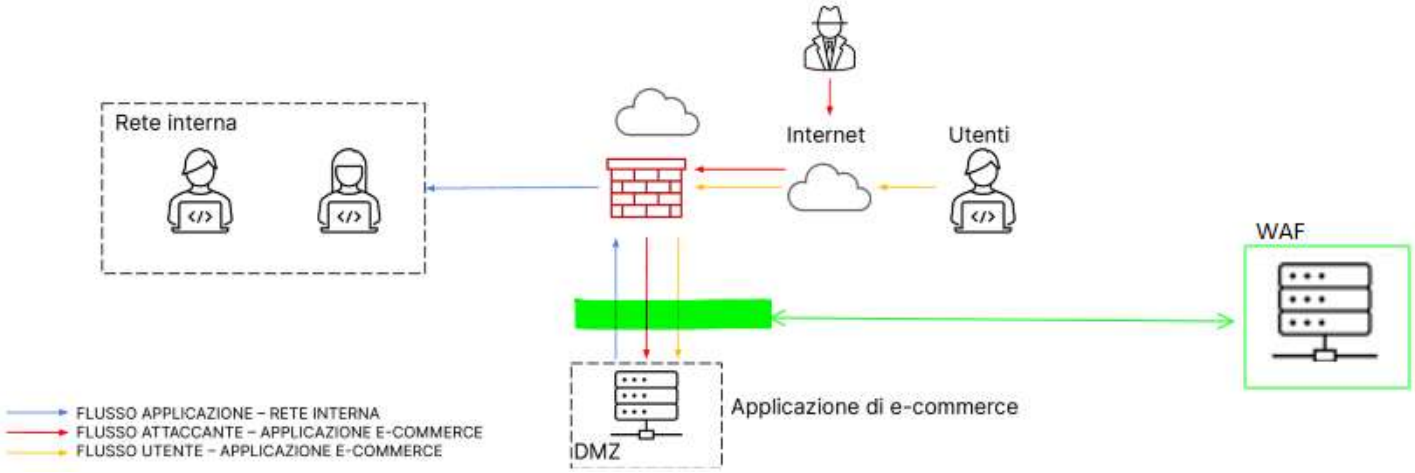


Esecuzione:

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?**

1) Assicurarsi che i dati immessi dagli utenti rispettino la sintassi richiesta, come lunghezza, formato e tipo di dati. Assicurarsi di pulire i caratteri speciali per evitare l'esecuzione di script non desiderati per previene gli attacchi XSS;
2) Utilizzare framework Web aggiornati che includano funzionalità di sicurezza, come la prevenzione automatica di SQL Injection e XSS;
3) Aggiornare con le patch di sicurezza più recenti tutti i software, sistema operativo, server Web, il database e framework utilizzato;
4) Configurare firewall, bloccare o filtrare le richieste che sembrano sospette;
5) Limitazione dei privilegi del database;
6) Tenere monitorato il sistema con log per rilevare attività sospette;

Pr aumentare il grado di sicurezza va implementare una Web Application Firewall (WAF) Firewall per il web, dove filtra il traffico e le richieste web.



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

Calcolo dell'impatto causa di un attacco DDoS:

-Impatto finanziario = Durata dell'interruzione (in minuti) * Perdita di guadagno per minuto
-Impatto finanziario = 10 minuti x 1.500 €/minuto
-Impatto finanziario = 15.000 €

Quindi, l'azienda ha perso 15.000 € a causa dell'attacco DDoS.
Più eventuali disservizi, non calcolabili come la rimessa in funzione dell'e-commerce (Ripristino backup) oppure un avvio del server secondario di backup per il ripristino delle macchine secondarie.

Per prevenire gli attacchi DDoS:
-Impostare limiti di traffico nel Firewall per controllare quante richieste può fare un utente in un certo periodo per evitare il sovraccarico del server;
-Usare strumenti di monitoraggio del traffico per individuare attività sospette e attivare avvisi tempestivi;
-Fare backup regolari e avere un piano di ripristino rapido, aiuta a ripristina in modo sicuro e veloce l'e-commerce;
-Mantenere i sistemi di sicurezza aggiornati e installare patch di sicurezza per proteggere l'applicazione da vulnerabilità note che potrebbero essere sfruttate per gli attacchi DDoS;

Implementare un Firewall IPS/IDS se l'azienda può permetterselo, oppure affidare l'e-commerce, a un'infrastruttura che offre servizi di questo tipo (datacenter che garantiscano protezione da questi attacchi, esempio www.cloudflare.com/it-it/ddos/ offre un servizio a pagamento, che permette di essere difesi in caso di attacco DDOS.)

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.

La priorità è impedire la propagazione del malware sulla rete senza interrompere l'accesso dell'attaccante alla macchina infettata.

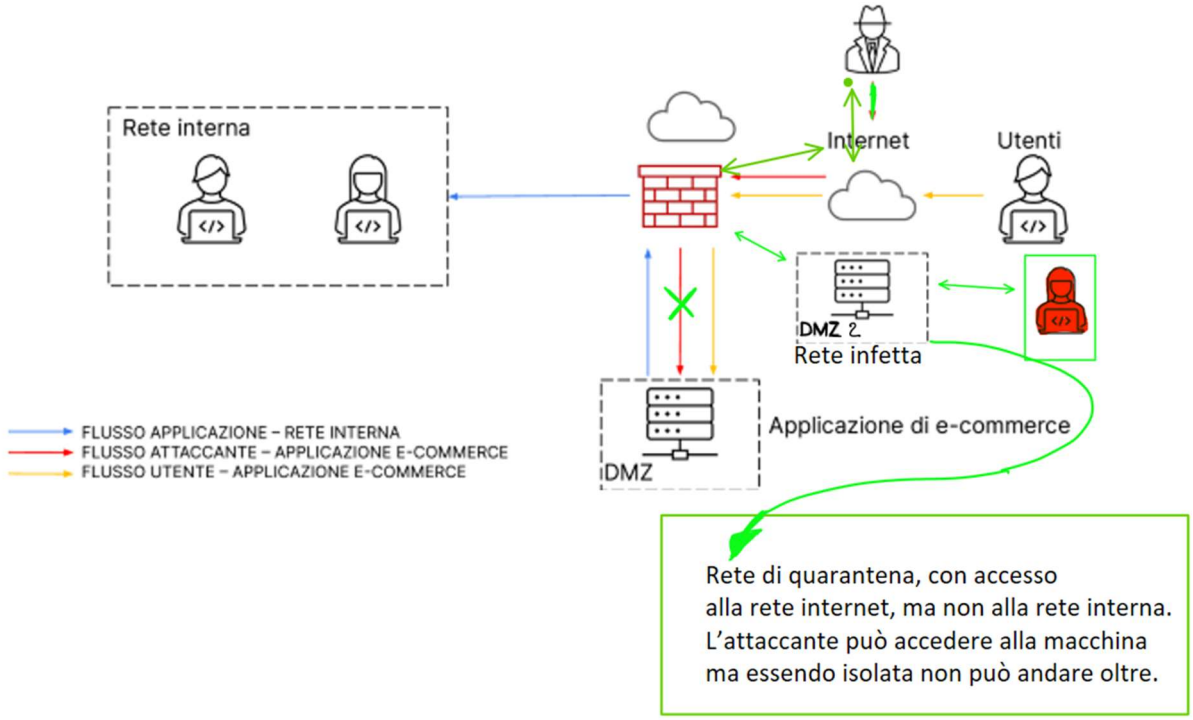
1) Isolare immediatamente la macchina infettata dalla rete principale utilizzando tecniche di segmentazione di rete (DMZ2 rete di quarantena).

2) Monitorare il traffico di rete e rilevare eventuali attività sospette o comportamenti anomali associati al malware.

3) Condurre un'analisi dettagliata del malware per comprendere il suo comportamento, le modalità di propagazione all'interno della rete e i vettori di attacco.

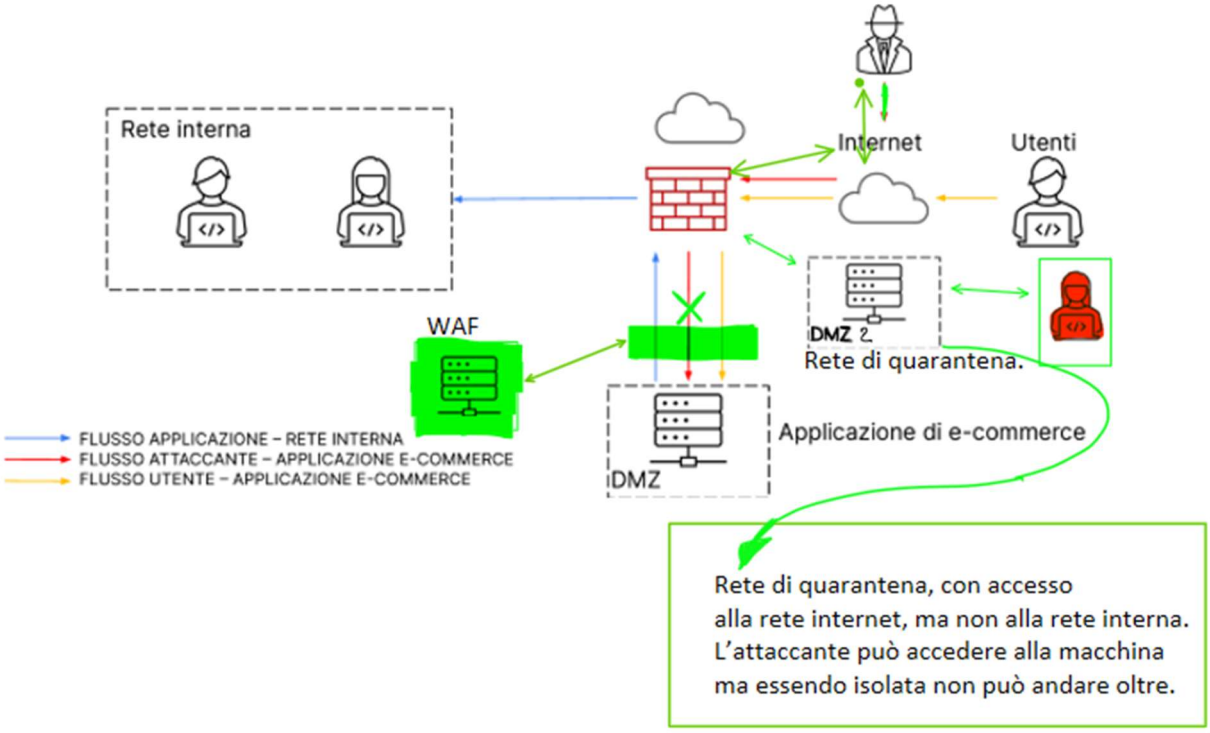
4) Potenziare le misure di sicurezza esistenti, come firewall, antivirus, filtri di ingresso e di uscita, per prevenire la diffusione del malware e bloccare eventuali tentativi di comunicazione con server di comando e controllo (questo solo nella rete DMZ1).

5) Aggiornare con le patch di sicurezza i sistemi/dispositivi, per ridurre la vulnerabilità agli attacchi e mitigare il rischio di futuri attacchi malware.



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

Implemento la soluzione del primo punto con il terzo, Inserisco il *Web Application Firewall (WAF)* del punto uno e inserisco la *rete di quarantena(DMZ2)* del punto 3.



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

Per una soluzione più aggressiva si può,

1) Rimuovere la macchina infetta;
2) Eseguire una scansione antivirus e malware approfondita dei sistemi attivi;
3) Analizzare il backup delle macchine per capire se è stato compromesso, ma se il lavoro è stato eseguito correttamente non ci dovrebbero essere problemi;
4) Aggiornare tutte le macchine, server, e applicazione con le ultime patch di aggiornamento;
5) Dove necessario resettare l'intera macchina così da evitare eventuali rischi per la rete;
6) Dove necessario resettare l'intero server e ripristinare le policy da un backup se quest'ultimo non è stato corrotto;
7) Avviare il tutto e aumentare il livello di sicurezza, tenendo monitorato tutto il traffico di rete, almeno per un certo periodo di tempo;
8) Implementare un firewall IPS/IDS dove possibile.
9) Creare campagne per formazione del personale;

Cybersecurity Analyst 2023-2024