Report W20D4 Benchmark 5

Redatto da: Pandolfi Luciano

Data: 28/01/25

Traccia:

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

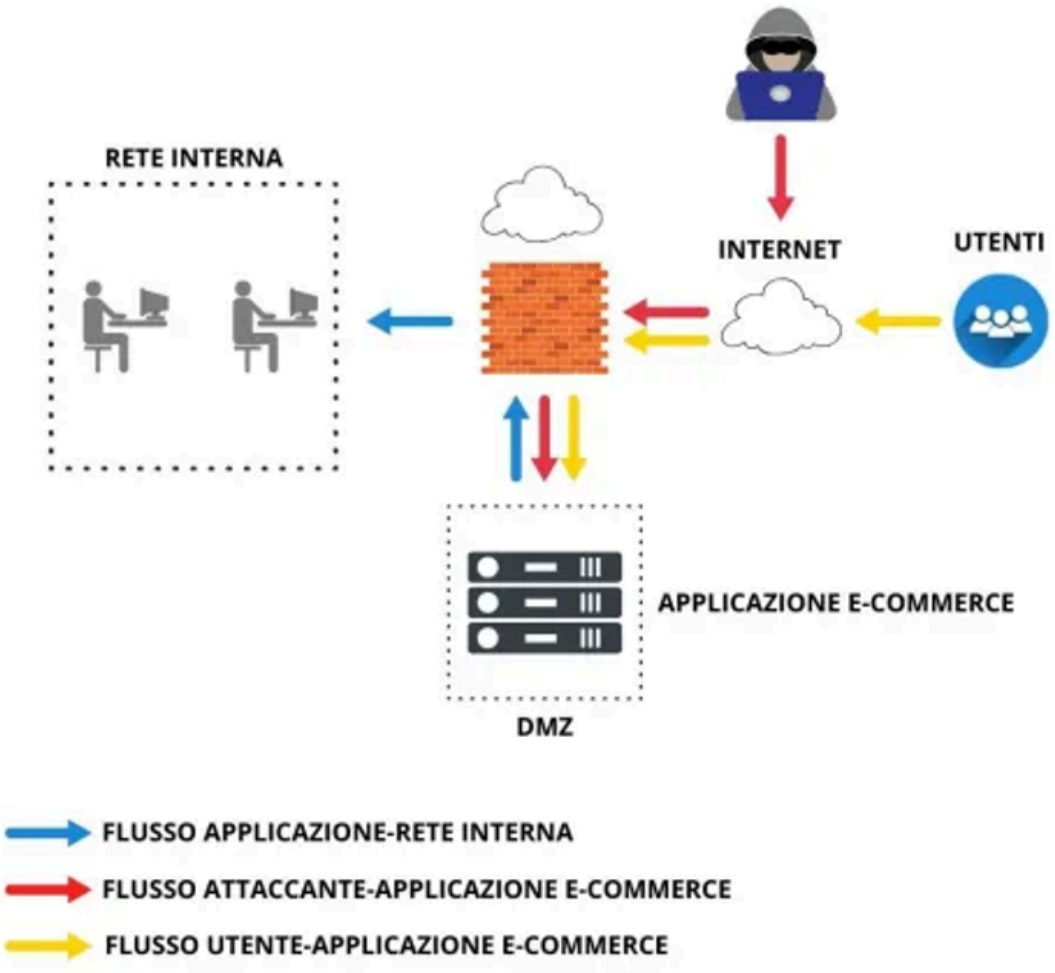
5. Modifica «più aggressiva» dell'infrastruttura (se necessario/facoltativo magari integrando la soluzione al punto 2).

Relazione sulla Sicurezza Informatica: Prevenzione, Impatto e Risposta agli Attacchi.

INDICE

SVOLGIMENTO

Situazione Iniziale



1. Azioni Preventive contro SQLi e XSS

Come misure di sicurezza aziendale potremmo implementare un Web Application Firewall (WAF) ed utilizzare strumenti di auditing come Burp Suite e SQLMap.

Invece, per difendere l'applicazione Web da attacchi di tipo SQL Injection (SQLi) e Cross-Site Scripting (XSS), si possono implementare altre azioni preventive:

1.1 Prevenzione SQL Injection

- Utilizzo di query parametrizzate;

- Validazione e sanitizzazione degli input utente;

- Implementazione di Object-Relational Mapping (ORM).

1.2 Prevenzione Cross-Site Scripting

- Escape dei dati in output;

- Implementazione di Content Security Policy (CSP);

- Sanitizzazione degli input HTML.

2. Impatto sul Business di un Attacco DDoS

L'applicazione Web ha subito un attacco DDoS che ha reso il servizio non raggiungibile per 10 minuti, considerando che in media ogni minuto gli utenti spendono 1.500 € sulla piattaforma di e-commerce, calcoliamo l'impatto economico:

Costo del Tempo di Inattività (CoD) = Guadagno per Minuto (GpM) x Tempo di Inattività (TdI) CoD = 1.500 € x 10 minuti = 15.000 €.

L'impatto economico diretto dell'attacco DDoS è stato di 15.000 €.

2.1 Azioni Preventive contro Attacchi DDoS

- Implementare sistemi di filtraggio del traffico e blocco IP (IDS E IPS);

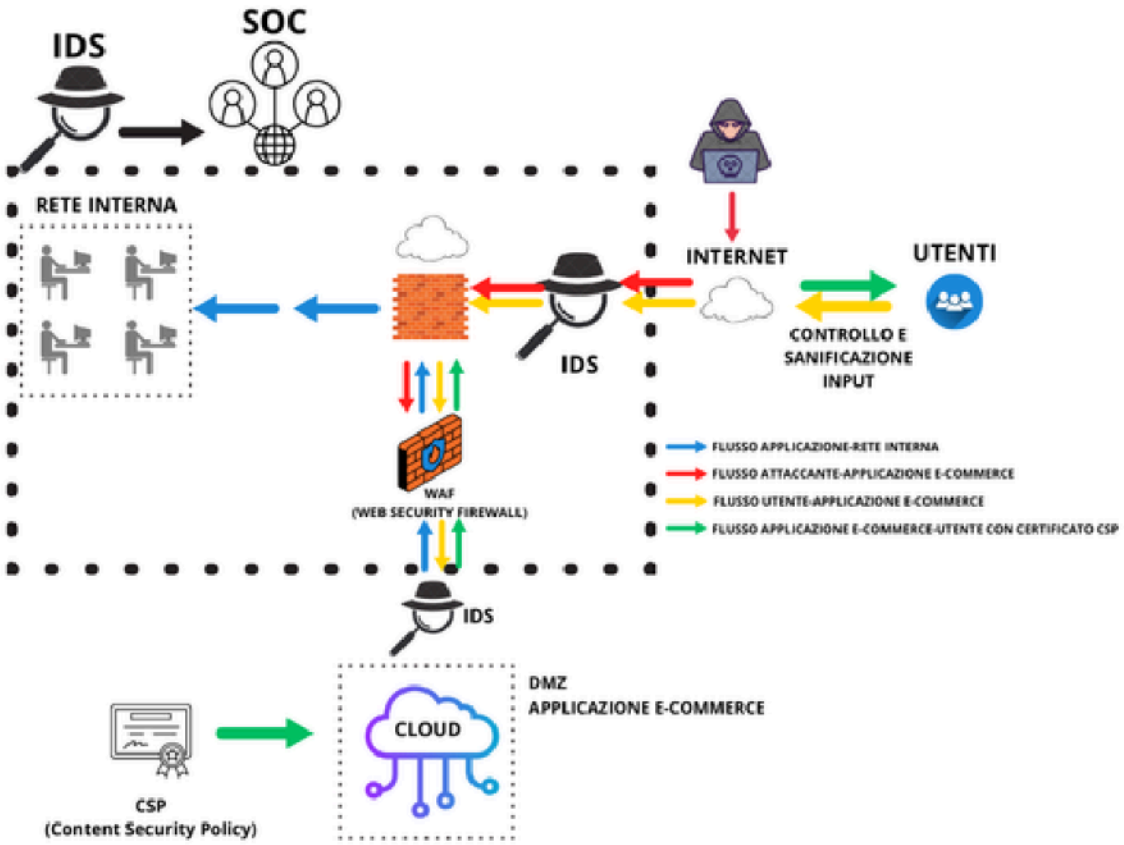
- Fare backup ricorrente dei dati;

- Implementare un'infrastruttura cloud per la sicurezza e la gestione delle memorie aziendali, garantendo una maggiore disponibilità del servizio agli utenti e assicurando una continuità operativa più rapida, grazie a backup e disaster recovery integrati.

- Introdurre il NAC (Network Access Control) come barriera di sicurezza che permette di gestire chi può entrare nella rete e con quali permessi.

- Eseguire lo scaling delle risorse server ed isolare la minaccia (VPC o VLAN).

Screen:



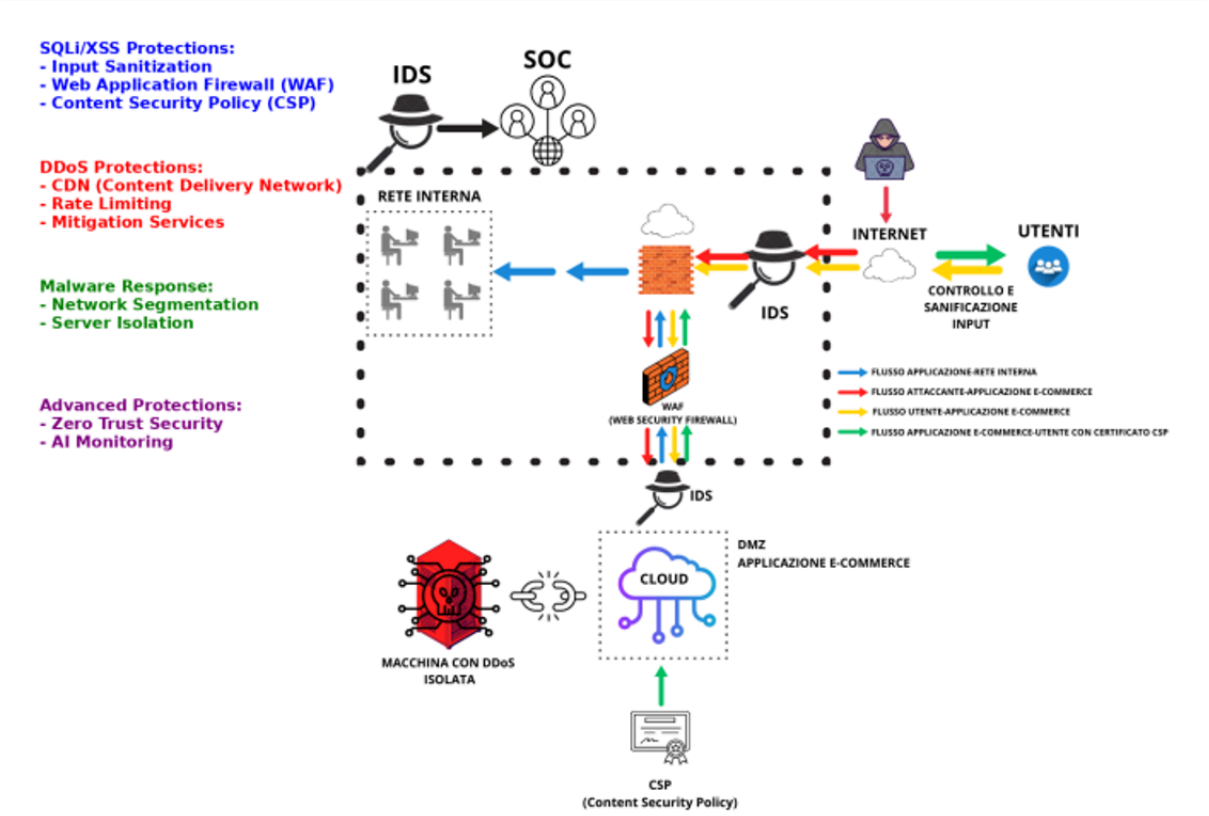
3. Response

La priorità è che il malware non si propaghi sulla nostra rete (interna), ecco alcune azioni di risposta che si potrebbero intraprendere:

- Isolare la macchina infetta utilizzando un Virtual Private Cloud o creando una VLAN di quarantena in modo da poter in seguito esaminare il malware in ambiente sandbox ed evitare che il problema si verifichi nuovamente;

- Monitorare il traffico di rete, identificando e bloccando comunicazioni sospette;

Screen:



4. Soluzione Completa di Sicurezza

Unendo le azioni preventive e di risposta, otteniamo una soluzione completa che include:

- Prevenzione di SQLi e XSS attraverso pratiche di codifica sicura e l'utilizzo del WAF;

- Mitigazione di attacchi DDoS attraverso l'utilizzo del CDN (Content Delivery Network) e sistemi di filtraggio avanzati;

- Isolamento e contenimento rapido della minaccia in caso di infezioni da malware;

- Monitoraggio continuo e analisi del traffico di rete.

5. Modifiche più Aggressive all'Infrastruttura

Per una protezione ancora più efficace, si potrebbero implementare le seguenti modifiche:

- Adottare un’architettura di rete completamente Zero Trust (verifica continua degli accessi/identità utente, minimizzazione dei privilegi e segmentazione della rete);

- Utilizzare honeypot per attirare e studiare potenziali attacchi;

- Implementare sistemi di Threat Intelligence per prevenire gli attacchi;

- Adottare soluzioni di sicurezza basate sull’ Intelligenza Artificiale e sulle Machine Learning.