SECURITY OPERATION

REPORT PROGETTO M5-W20D4

Federica Di Fiore
Cybersecurity Analyst PT

Indice

Il presente report analizza la sicurezza di un'infrastruttura e-commerce esposta su Internet, partendo da una serie di scenari pratici proposti nel modulo formativo.
Attraverso risposte tecniche mirate, vengono approfondite le azioni preventive contro attacchi come SQLi, XSS e DDoS, le strategie di contenimento malware, e le soluzioni architetturali utili a rafforzare il perimetro.
Lo scopo è fornire una visione chiara e applicabile dei principali rischi e delle relative contromisure in ambito Web Application Security e Network Defense.

1. AZIONI PREVENTIVE

Per prevenire attacchi SQL Injection (SQLi) e Cross-Site Scripting (XSS), è fondamentale adottare una serie di contromisure tecniche e procedurali, sia a livello di codice che di infrastruttura. Di seguito le principali azioni preventive:

- Validazione e sanitizzazione degli input: ogni dato proveniente da utenti esterni deve essere filtrato per evitare caratteri malevoli. Ad esempio, si devono rimuovere o codificare caratteri speciali e HTML.
- Utilizzo di query parametrizzate (prepared statements): per prevenire SQLi, è essenziale separare i dati dalle istruzioni SQL.
- WAF (Web Application Firewall): implementare un WAF in grado di rilevare e bloccare attacchi XSS/SQLi noti grazie a regole preconfigurate.
- Aggiornamenti e patch: mantenere il CMS, i plugin e le librerie sempre aggiornati per evitare vulnerabilità note.
- HTTP security headers: come Content-Security-Policy, X-Content-Type-Options, X-XSS-Protection ecc.

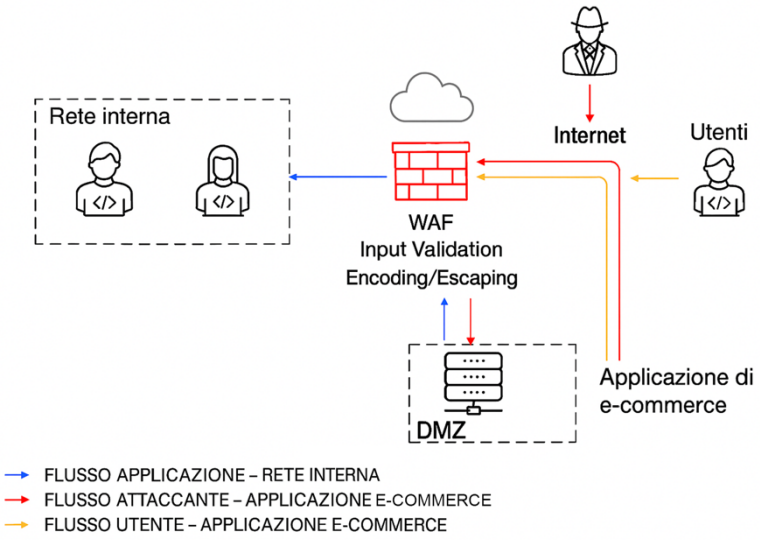

Figura 1 L'illustrazione mostra l'uso di un WAF con validazione degli input ed encoding per bloccare attacchi dannosi prima che raggiungano l'applicazione di e-commerce nella DMZ.

2. IMPATTI SUL BUSINESS

Durante un attacco DDoS, l'applicazione e-commerce risulta irraggiungibile per 10 minuti. Con una media di €1.500 spesi al minuto, l'impatto diretto sul business è:

€1.500 x 10 min = €15.000 di perdita diretta

Oltre alla perdita economica immediata, si aggiungono impatti indiretti quali:

- Perdita di fiducia da parte degli utenti;
- Possibile danno reputazionale;
- Costi di supporto e assistenza clienti;
- Rischi di abbandono del carrello o dei pagamenti

AZIONI CONSIGLIATE:

- CDN con protezione DDoS integrata (es. Cloudflare, Akamai);
- Rate limiting e throttling sulle richieste;
- WAF con regole anti-DDoS;
- Architettura scalabile con bilanciamento del carico;
- Monitoring e alerting in tempo reale

3. RESPONSE

Nel caso in cui l'applicazione venga compromessa da un malware, l'obbiettivo prioritario è evitare la propagazione del codice malevolo alla rete interna, anche se l'accesso dell'attaccante alla macchina infetta non viene rimosso.

AZIONI DI CONTENIMENTO:

- Segmentazione della rete: separare logicamente la DMZ dalla rete interna tramite firewall con regole restrittive;
- Isolamento del server compromesso: bloccare ogni comunicazione tra la macchina infetta e la rete interna (ad esempio, usando ACL sul firewall);
- Monitoraggio del traffico in uscita per identificare eventuali movimenti laterali o comunicazioni con C2 (Command & Control);
- Registro e logging: acquisire log per analizzare il comportamento del malware e preparare la fase di recovery.

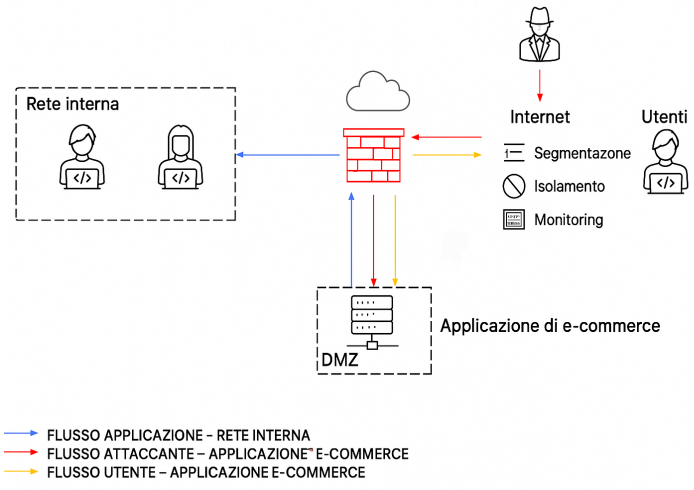

Figura 2 La rete è segmentata e l'applicazione di e-commerce isolata nella DMZ. Il traffico è monitorato, limitando la superficie d'attacco e migliorando la visibilità sugli accessi sospetti.

4. SOLUZIONE COMPLETA

La soluzione completa prevede l'unione delle misure di prevenzione (contro SQLi/XSS) e delle azioni di risposta (malware containment) in un'unica infrastruttura di difesa.

ELEMENTI INTEGRATI:

- Input validation + query parametrizzate;
- WAF configurato per bloccare attacchi comuni;
- Headers HTTP sicuri;
- Firewall che isola DMZ dalla rete interna;
- Logging centralizzato e monitoraggio in tempo reale
- CSP: Content Security Policy

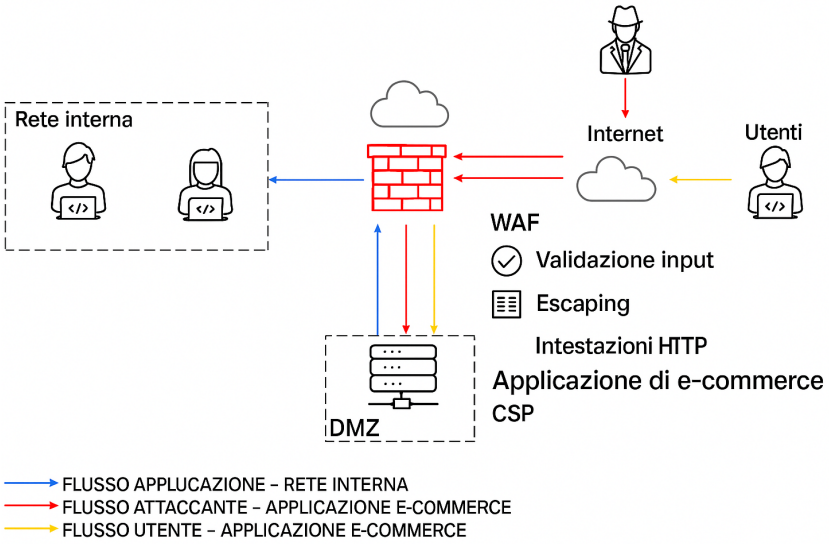

Figura 3 L'applicazione e-commerce è protetta da un WAF, validazione degli input, escaping e intestazioni HTTP (inclusa CSP), per contrastare minacce come XSS e injection.

5. MODIFICA PIU' AGGRESSIVA DELL'INFRASTRUTTURA

Per aumentare ulteriormente la sicurezza, si può proporre una modifica più incisiva all'infrastruttura esistente, introducendo un approccio Zero Trust e migliorando la visibilità e il controllo del traffico.

PROPOSTE:

- Bastion Host: per l'accesso controllato alla DMZ e ai sistemi interni;
- Reverse Proxy con autenticazione a più fattori per gli accessi amministrativi;
- Rete interna protetta da un IDS/IPS per rilevare attività sospette;
- Microsegmentazione: ogni servizio della rete isolato in sottoreti con ACL specifiche;
- Monitoraggio continuo + SIEM per aggregare log e correlare eventi in tempo reale;
- VPN IPsec per accesso remoto sicuro da parte degli amministratori.

Questa modifica riduce al minimo l'impatto di eventuali compromissioni, aumentando la resilienza dell'intera architettura.

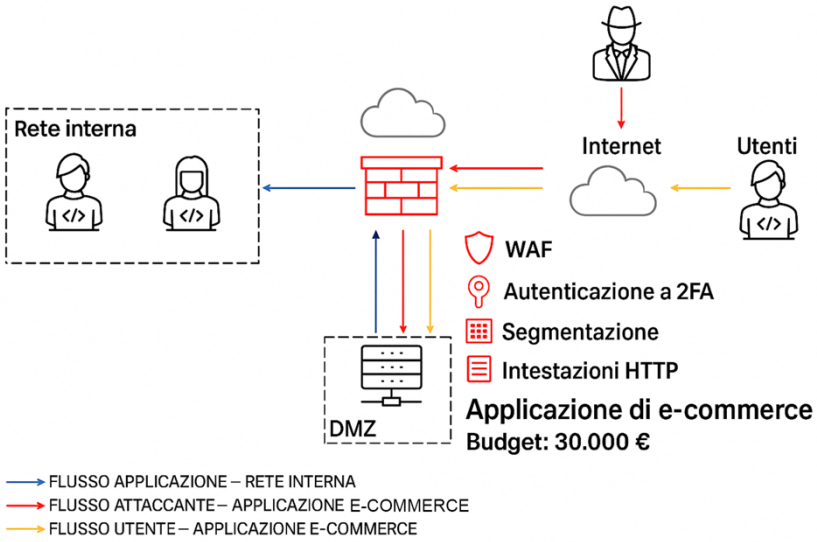

Figura 4 La segmentazione, l'isolamento dei servizi e il monitoraggio continuo riflettono un approccio Zero Trust, in cui ogni componente viene controllato e verificato per limitare i movimenti laterali e ridurre l'impatto di eventuali compromissioni.

UTILIZZO STRATEGICO DI UN BUDGET PER MODIFICA AGGRESSIVA

Dato un budget complessivo di 30.000 euro, verrà impiegato in modo mirato per rafforzare i sistemi critici, migliorare la capacità di rilevamento e risposta, e aumentare la resilienza dell'intero perimetro IT.

INVESTIMENTI CHIAVE E RIPARTIZIONE DEL BUDGET:

1. **Firewall di nuova generazione e WAF avanzato – circa 7.000 €**

   Il primo intervento prevede l'introduzione di un **WAF (Web Application Firewall)** con funzioni di **machine learning e threat intelligence** in tempo reale, capace di analizzare i pattern di traffico web e bloccare in automatico richieste malevole, come attacchi SQLi, XSS e tentativi di accesso non autorizzato. Questo strumento sarà configurato per proteggere attivamente la **web application di e-commerce**.

2. **Segmentazione di rete e hardening della DMZ – circa 5.000 €**

   Si procederà con l'implementazione di **VLAN** e firewall interni per segmentare i vari ambienti (frontend, backend, database) riducendo il movimento laterale in caso di compromissione. La zona **DMZ** verrà sottoposta a **hardening sistemistico**, limitando le superfici di attacco e applicando criteri di accesso minimali.

3. **Sistema SIEM e monitoraggio centralizzato – 6.000 €**

   Per ottenere una visione globale degli eventi e individuare rapidamente attività sospette, verrà adottato un **SIEM** in grado di raccogliere, normalizzare e correlare i log di rete, server, firewall e WAF. Il sistema sarà configurato per inviare **alert automatici** e report periodici al Security Team.

4. **Autenticazione multifattoriale (MFA) – 3.000 €**

   Per rafforzare il sistema di accesso ai pannelli di gestione dell'e-commerce e ai server backend, sarà implementata un'autenticazione forte tramite **MFA (Multi-Factor Authentication)**, che combinerà credenziali tradizionali con codici temporanei generati da app o dispositivi hardware.

5. **Vulnerability Assessment e Penetration Testing – 4.500 €**

   Al fine di verificare l'efficacia delle misure introdotte, verranno eseguite **attività di VA/PT** da parte di un team esterno qualificato, che simulerà scenari d'attacco realistici. I risultati verranno analizzati per identificare eventuali ulteriori lacune.

6. **Integrazione di un sistema SOAR – 2.000 €**

   Per automatizzare le risposte agli alert più comuni generati dal SIEM, verrà integrata una piattaforma **SOAR**. Essa consentirà di creare **playbook** di risposta per incidenti ricorrenti (es. brute-force, scansioni di rete, comportamenti anomali), riducendo i tempi di intervento e il carico operativo sul team SOC. Il SOAR permetterà anche l'esecuzione automatica di task come **isolamento host**, **revoca di credenziali** e **notifica ai responsabili.**

7. **Formazione tecnica del personale – 2.500 €**

   Ultimo ma non meno importante, parte del budget sarà impiegato per **formare il personale** in materia di sicurezza applicativa (con focus su OWASP Top 10), gestione sicura delle patch, e procedure di risposta a incidenti. Una risorsa formata è il primo strato di difesa.

CONCLUSIONE

L'intervento di **modifica aggressiva**, supportato da un budget di 30.000 euro, rappresenta un investimento strategico orientato alla **prevenzione avanzata, alla visibilità continua e alla risposta efficace agli attacchi**. L'obiettivo non è soltanto mitigare le vulnerabilità esistenti, ma creare un **ecosistema resiliente**, capace di adattarsi alle minacce future e garantire la **continuità operativa** del servizio e-commerce. Questo approccio bilancia **tecnologia, processo e formazione**, elementi chiave per un framework di sicurezza moderno e sostenibile.