Operazioni di sicurezza
Epicode - Azioni preventive
Calcolo impatto

Giuseppe Gigliotti - gius199874@gmail.com

3 dicembre 2025

Indice

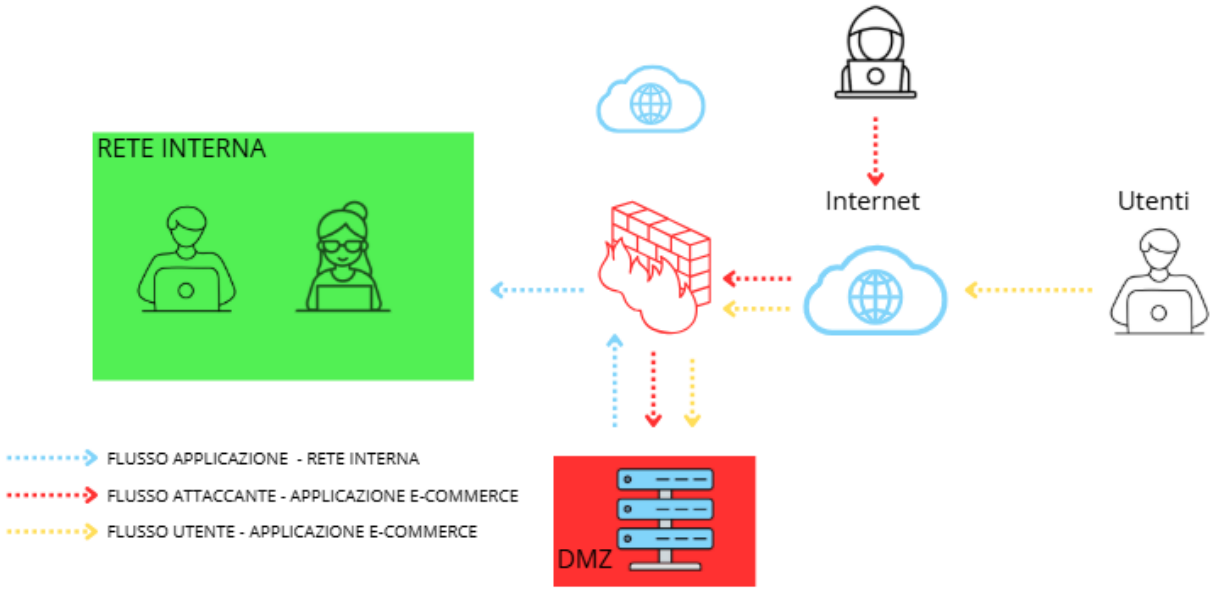


Figura 1: Architettura iniziale

Riassunto Esecutivo:

Con riferimento alla figura, rispondere ai seguenti quesiti.

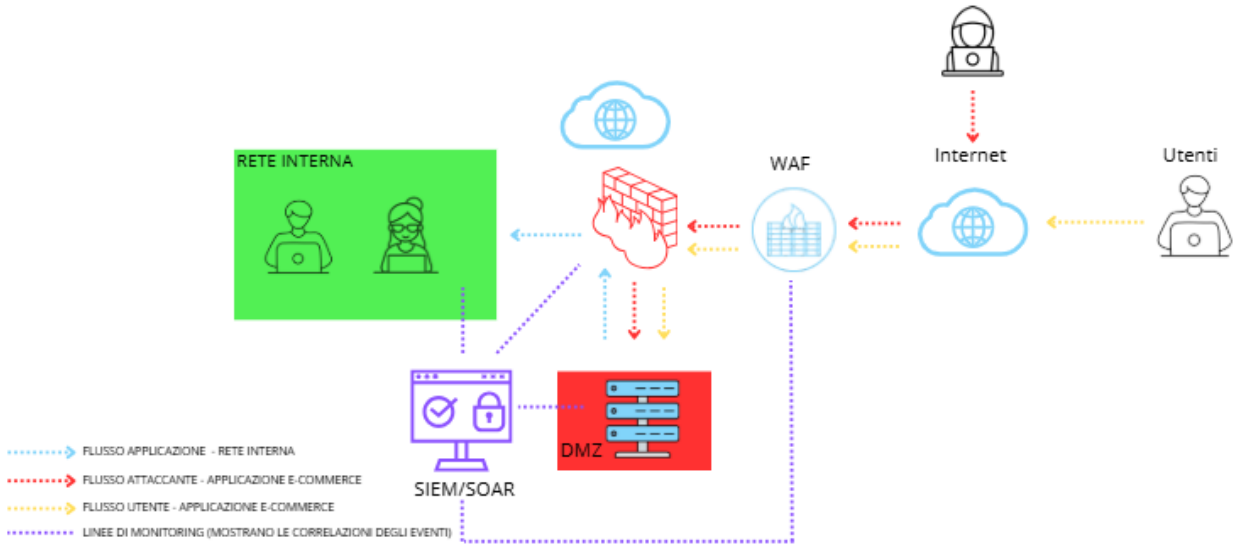
1. Azioni preventive: quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni
2. Impatti sul business: l'applicazione Web subisce un attacco 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)

Scopo del test:

1. Azioni preventive:

Per SQL Injection e Cross-Site Scripting (XSS):

Per la protezione della Web App da minacce quali XSS e SQLi si può preventivamente adottare una soluzione basata su Web Application Firewall (WAF), che a differenza dei firewall standard, sono dedicati per proteggere le Web App da attacchi XSS e SQLi. La figura iniziale si modifica di conseguenza come la figura di seguito, dove abbiamo ipotizzato che il WAF sia a protezione del traffico in entrata sulla Web App da internet (quindi utenti e attaccante). La soluzione potrebbe prevedere l'inserimento di un SIEM/SOAR che riceva informazioni in input dalla rete interna,firewall, WAF e DMZ.



2. Impatto sul business:

Calcolo dell'impatto:

L'applicazione Web ha subito un attacco DDoS che l'ha resa non raggiungibile per 10 minuti.

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 €.

Azioni preventive DDoS:

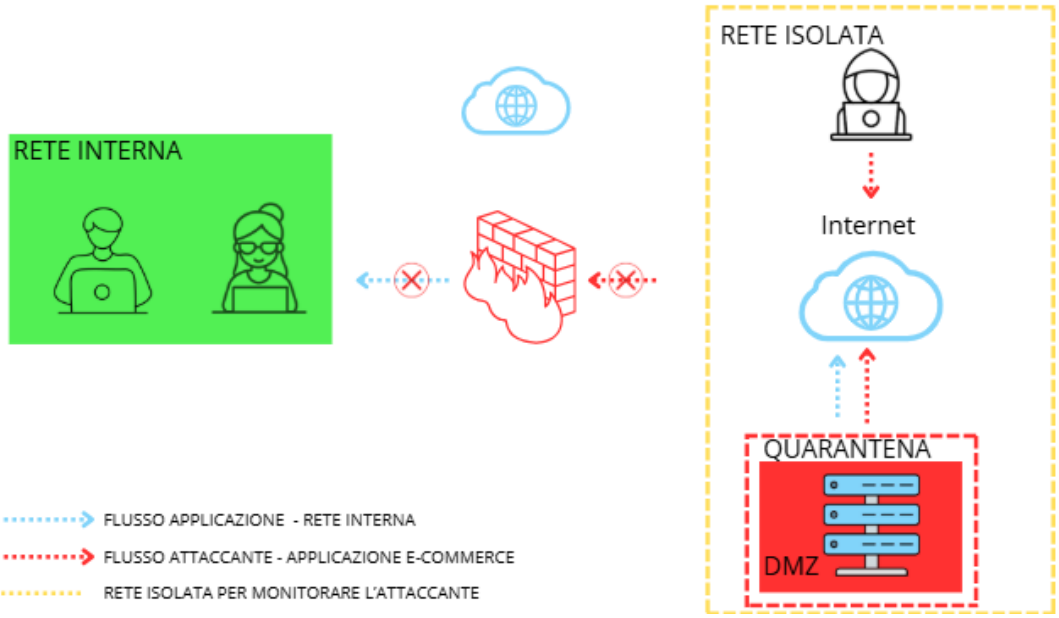
- CDN con protezione DDoS (es. Cloudflare, Akamai)

- Rate Limiting sul firewall/WAF
- Auto-scaling dell'infrastruttura
- Servizi anti-DDoS specializzati
- Network filtering a livello ISP

3. Response:

Per impedire la propagazione senza rimuovere l'attaccante:

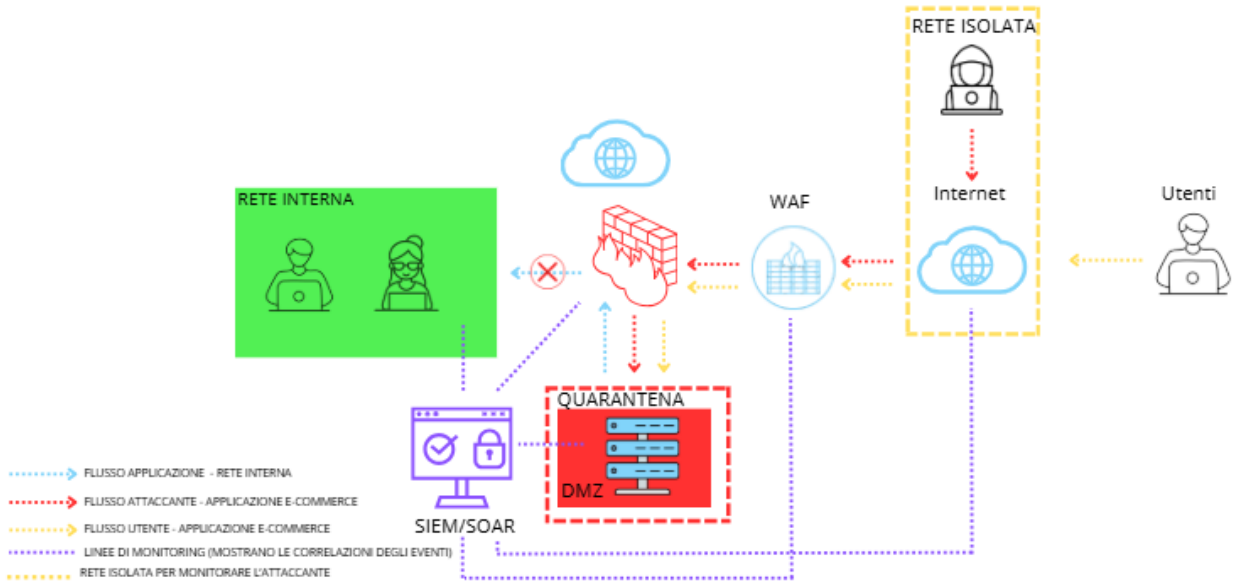
Considerata la priorità, si può adottare una strategia basata sull'isolamento della macchina infettata. In questo caso la macchina sarà direttamente collegata ad internet, raggiungibile dall'attaccante ma non più connessa alla rete interna. La figura mostra la soluzione con la strategia dell'isolamento della macchina infetta. Possiamo notare come non ci sia più comunicazione tra l'applicazione Web e la rete interna.



4. Soluzione completa:

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

- Prevenzione di SQLi e XSS attraverso pratiche di codifica sicura e WAF
- Isolamento e contenimento rapido in caso di infezioni da malware
- Monitoraggio continuo e analisi del traffico di rete


RETE ISOLATA
Internet
Utenti
WAF
RETE INTERNA
QUARANTENA
DMZ
SIEM/SOAR
FLUSSO APPLICAZIONE - RETE INTERNA
FLUSSO ATTACCANTE - APPLICAZIONE E-COMMERCE
FLUSSO UTENTE - APPLICAZIONE E-COMMERCE
LINEE DI MONITORING (MOSTRANO LE CORRELAZIONI DEGLI EVENTI)
RETE ISOLATA PER MONITORARE L'ATTACCANTE