Report di Sicurezza
Architettura eCommerce

Analisi delle vulnerabilità, contromisure preventive e risposta agli attacchi informatici

Data: 12/07/2025

M5

W20D4

Report Completo
Architettura di Sicurezza
E-commerce

Traccia

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

1. **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**

1. **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.

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

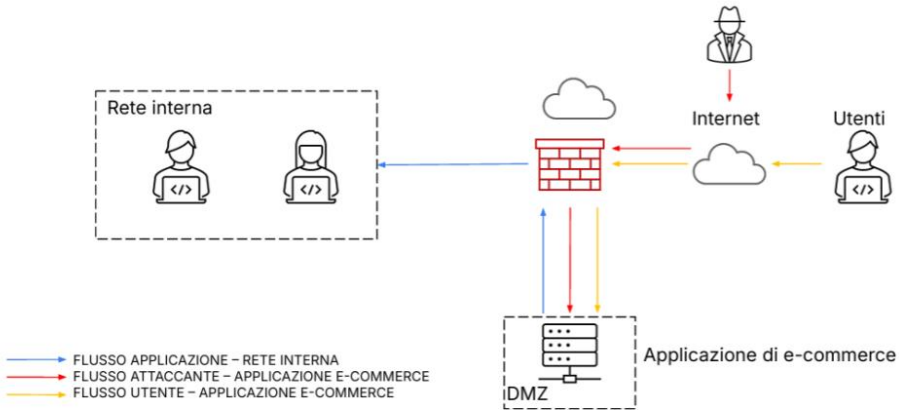
1. **Modifica «più aggressiva» dell'infrastruttura (se necessario/facoltativo magari integrando la soluzione al punto 2)**

3

Architettura Iniziale

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.

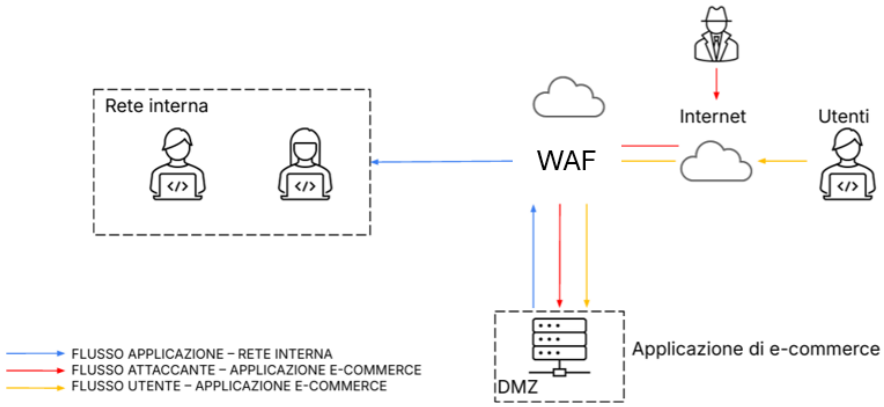


4

1. Azioni preventive (SQLi/XSS)

Per proteggere l'applicazione Web da attacchi SQLi e XSS:
- Utilizzo di query parametrizzate per evitare SQL Injection, invece di inserire direttamente I dati dell'utente all'interno di una query SQL si usano segnaposto che vengono riempiti in modo sicuro dal database.
- Validazione e sanitizzazione degli input Utente, verificare che I dati inseriti dall'utente siano corretti, complete e nel formato corretto e pulire l'imput da caratteri potenzialmente pericolosi.
- Escaping dell'output nei contenuti HTML e JavaScript, trasformando I caratteri speciali che potrebbero essere interpretati come codice eseguibile in simboli innocui.
- Implementazione di una Content Security Policy (CSP), definire e applicare una **politica di sicurezza** che dice al browser **quali contenuti può caricare e da dove.**
- Impiego di un Web Application Firewall (WAF) per analizzare e bloccare traffico sospetto, mettere un sistema di sicurezza **tra gli utenti e l'applicazione web**, che **analizza il traffico in tempo reale** e blocca automaticamente richieste **malintenzionate o sospette**

La figura evidenzia l'inserimento del WAF tra Internet e DMZ e i controlli a livello applicativo nella rete interna.



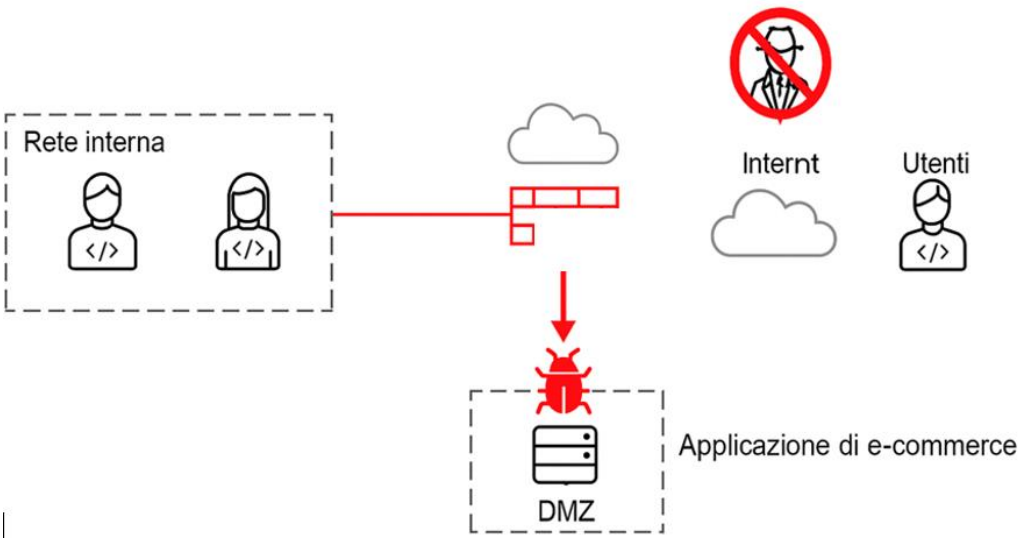
2. Impatti sul business (DDoS)

L'applicazione subisce un attacco DDoS dall'esterno, che la rende inaccessibile per 10 minuti.
Con una media di spesa di 1.500 EUR al minuto, la perdita economica è:

1.500 EUR/min x 10 min = 15.000 EUR

Azioni preventive consigliate:
- Protezione anti-DDoS tramite servizi come Cloudflare, AWS Shield, ecc., bloccando il traffico prima che raggiunga il server (DMZ), filtrando quello malevolo e lasciando passare quello legittimo.
- Rete limiting e challenge (CAPTCHA, JS Challenge), limitando il numero di richieste fatte dall'utente in determinato periodo di tempo.
- CDN per contenuti statici e scalabilità automatica, utilizzando una rete di server distribuiti in varie parti del mondo che ospitano copie dei contenuti (pdf, immagini, video, ecc.) per ridurre tempi di caricamento e carico sul server principale e scalabilità automatica aggiunge e toglie le risorse in base all'utilizzo richiesto per evitare che il sito crolli e gestisce carichi elevate senza down time.

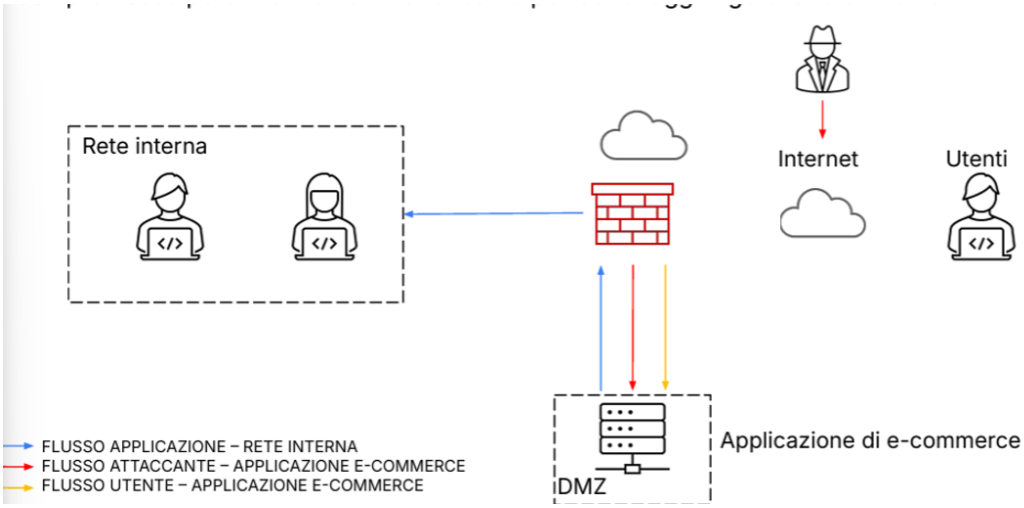
La figura aggiornata mostra un filtro di protezione DDoS davanti all'infrastruttura.



3. Response (infezione malware)

Nel caso di infezione malware nel server DMZ:
- La priorità è impedire la propagazione verso la rete interna.
- Si blocca ogni comunicazione in uscita dalla DMZ.
- Il traffico in ingresso dall'Internet rimane attivo, così l'attaccante può mantenere il controllo.

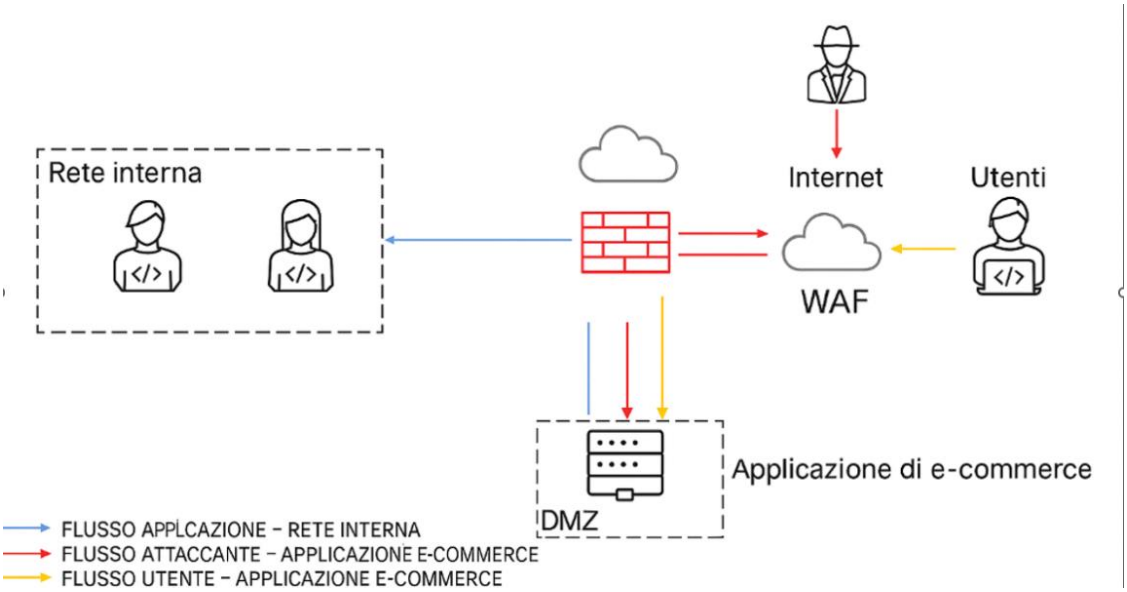
La figura rappresenta chiaramente il blocco del flusso tra DMZ e rete interna e l'isolamento della macchina.



4. Soluzione completa (preventiva + response)

Unendo le due soluzioni:
- Il WAF (Web Application Firewall) protegge l'applicazione da SQLi, XSS, DDoS, potendo intercettare, analizzare e bloccare richieste malevole prima che arrivino a destinazione.
- L'applicazione è sviluppata con controlli sicuri, utilizzando librerie aggiornate per le vulnerabilità note, aggiornamenti regolari, le azioni importanti vengono tracciate e registrate.
- La rete è segmentata e la DMZ isolata per contenere eventuali infezioni, limitando la propagazione di un attacco, controllare il traffico tra le varie zone della rete.

La figura mostra la difesa in profondità e la segmentazione della rete.



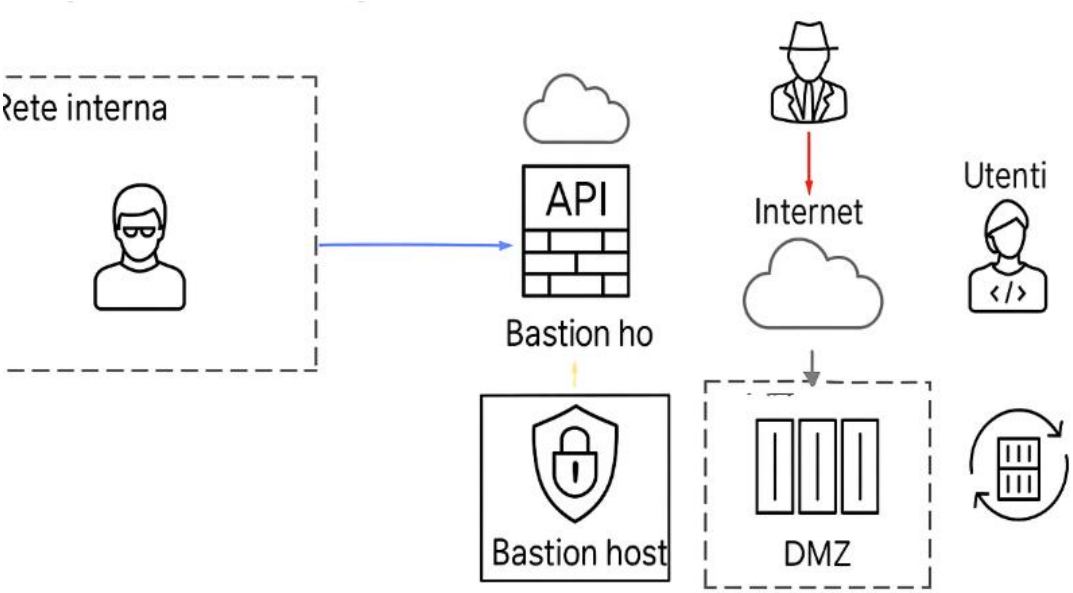
5. Modifica più aggressiva dell'infrastruttura

Si propone una rete Zero Trust:
- Nessuna comunicazione diretta dalla DMZ alla rete interna.
- Uso di proxy/API gateway per ogni accesso ai backend, dove nessun client o servizio comunica direttamente con I sistemi interni, ma passa da un punto centrale di controllo.
- Microsegmentazione e VLAN per ogni componente, andando quindi a creare dei compartimenti stagni, isolate e controllati.

- Bastion host con autenticazione MFA per accessi amministrativi, dove per entrare come amministratore si deve dimostrare di esserlo essendo sotto controllo.
- Immagini immutabili e rigenerazione dei container, dove se serve cambiare qualcosa non si modifica ma lo si termina e ne inizia uno nuovo basto sull'immagine aggiornata (pe immagine si intende un pacchetto che comprende il codice dell'applicazione, le librerie

necessarie, il Sistema operativo ecc.).

Questa soluzione riduce al minimo il rischio e limita drasticamente l'impatto in caso di compromissione.



5bis. Modifica più aggressiva dell'infrastruttura

Con budget prefissato di 20.000€ per implementare la sicurezza e prevenzioni da attacchi malware.

Obiettivi della modifica:

1. **Isolare la rete interna dalla DMZ**
2. **Proteggere l'applicazione da attacchi come XSS, SQLi, DDoS**
3. **Gestire gli accessi amministrativi in modo sicuro**
4. **Monitorare e loggare il traffico**
5. **Evitare modifiche manuali in produzione**

INFRASTRUTTURA SICURA – SOLUZIONE PROPOSTA

Architettura modificata:

- Inserimento di un **API Gateway/Reverse Proxy**
- Isolamento completo della rete interna (**niente più traffico diretto dalla DMZ**)
- Uso di **WAF + CDN + Anti-DDoS**
- **Bastion Host** per accessi admin
- Immagini immutabili e container rigenerabili
- Logging centralizzato e alerting

SOLUZIONI REALI CONSIGLIATE

Area	Soluzione reale	Costo stimato annuo	Descrizione breve
WAF + Anti-DDoS	Cloudflare Pro o Business	~240 €/anno (Pro), ~2.400 €/anno (Business)	Protezione SQLi, XSS, bot, DDoS, JS Challenge
API Gateway	NGINX Plus o Kong Gateway	~2.000 €/anno	Gestione traffico API, rate limiting, routing, logging
CDN globale	Incluso in Cloudflare o AWS CloudFront	Incluso nei piani	Riduce latenza e protegge dai flood
Bastion Host	AWS EC2 Bastion + MFA IAM	~600 €/anno	Accesso SSH limitato + autenticazione a più fattori
Containerization	Docker + Portainer + GitHub Actions CI/CD	Gratis (open-source)	Build automatizzati di immagini immutabili
Logging + Alerting	Grafana + Loki o [ELK Stack (Elastic)]	~0–1.000 €/anno	Tracciamento eventi di sicurezza e anomalie
Segmentazione di rete	VLAN su firewall/router (es. Ubiquiti UniFi)	~1.500 € (una tantum)	Isolamento per DMZ, utenti, backend
Monitoring	Zabbix, Prometheus	Gratis (open-source)	Monitoraggio stato servizi e anomalie

---

BUDGET TOTALE STIMATO

Componente	Costo
Cloudflare Business	2.400 €
Kong Gateway (2 istanze)	2.000 €
Bastion Host (AWS EC2 + storage + MFA)	600 €
Container e CI/CD	0 €
Logging & Alerting	1.000 € max
Ubiquiti + VLAN	1.500 € (una tantum)
Totale stimato primo anno	**~7.500 – 9.000 €**

Rimangono **~11.000 €** nel budget per:

- Extra istanze cloud
- Backup
- Formazione sicurezza
- Penetration test