REPORT TECNICO – SICUREZZA INFRASTRUTTURA E-COMMERCE

Cliente: Nencini Sport S.P.A
Data: 10/07/2025
Consulente di sicurezza informatica: Andrea Giovannoni

Parte 1 – Executive Summary (per l'Amministrazione)

Contesto e obiettivo

L'applicazione e-commerce aziendale, essendo esposta su Internet, è soggetta a numerosi rischi informatici. Questo report analizza tre scenari critici:

1. Prevenzione contro attacchi SQLi/XSS.
2. Impatto economico e tecnico di un attacco DDoS.
3. Contenimento di un'infezione malware.

L'obiettivo finale è proporre una **soluzione integrata**, professionale e sostenibile per ridurre i rischi e rafforzare la resilienza dell'infrastruttura, secondo i principi della **Cyber Resilience** e della **Zero Trust Architecture**.

Rischio 1: Attacchi applicativi SQLi / XSS

Gli attacchi alle vulnerabilità del codice (iniezioni SQL, script malevoli XSS) possono compromettere la riservatezza dei dati, causare danni alla reputazione o furti d'identità.

Soluzione proposta: protezione multilivello tramite:

- Validazione e sanitizzazione degli input a livello di codice.
- Uso di **WAF** (Web Application Firewall).
- Policy CSP (Content Security Policy).

- Header di sicurezza lato HTTP (X-Frame-Options, X-Content-Type-Options).

Rischio 2: Attacco DDoS – Impatto sul business

Un attacco di tipo DDoS ha reso indisponibile l'applicazione per **10 minuti**. Considerando che il sito genera **1.500 € al minuto**, il danno diretto stimato è:

Totale perdita: **10 min × 1.500 € = 15.000 €**

Soluzione proposta:

- Integrazione con una **CDN con protezione anti-DDoS** (es. Cloudflare, Akamai).
- **Rate Limiting** lato firewall.
- **Scrubbing service** esterni per filtrare traffico volumetrico.
- Configurazione di un **SIEM per alerting in tempo reale**.
- Analisi del **MTTR (Mean Time to Recovery)** per monitorare i tempi di reazione.

Rischio 3: Infezione malware

Nel caso di infezione da malware sulla Web App, la priorità è **contenere l'infezione** evitando la propagazione laterale verso la rete interna.

Soluzione proposta:

- **Segmentazione rigorosa della rete** tra DMZ e rete interna.
- Impiego di **IDS/IPS** tra zone di rete (es. Snort, Suricata).
- Isolamento automatico tramite **EDR** (es. CrowdStrike, SentinelOne).
- Disconnessione automatica dell'host compromesso (Network Quarantine).
- Logging centralizzato su **SIEM**, automatizzabile con **SOAR**.

Soluzione unificata

È essenziale integrare **prevenzione + risposta** in un'unica architettura resiliente.
Ciò include:

- WAF, CSP, Header Sicurezza
- IDS/IPS + SIEM
- EDR con isolamento automatico
- **Bastion Host** per accesso controllato alla DMZ
- **Backup cifrati off-site**
- Segmentazione e politica di accesso Zero Trust
- **Playbook di Incident Response** secondo MITRE ATT&CK

Parte 2 – Sezione Tecnica Dettagliata

1. Azioni preventive (SQLi/XSS)

Rischio	Tecnica di mitigazione	Tool/Soluzione
SQL Injection	Prepared Statements, ORM	SQLAlchemy, Django ORM
XSS	Output Encoding, CSP, Validazione	OWASP CRS, ModSecurity, CSP header
Header Sicurezza	Protezione base su tutti i browser	X-Frame-Options, X-XSS-Protection

WAF	Protezione Layer 7	AWS WAF, Cloudflare, ModSecurity
Scanner automatici	Rilevamento vulnerabilità	OWASP ZAP, Nikto, Burp Suite

---

2. Attacco DDoS – Impatto e mitigazioni

- **Danno diretto stimato**: **15.000 €** per 10 minuti
- **Azioni preventive**:
    - CDN con protezione DDoS
    - Scrubbing Center (es. Arbor Cloud)
    - Limiti di connessioni/IP
    - Monitoraggio SIEM per soglie di traffico
    - Aggiunta di un **SOC di 1° livello** per escalation rapida

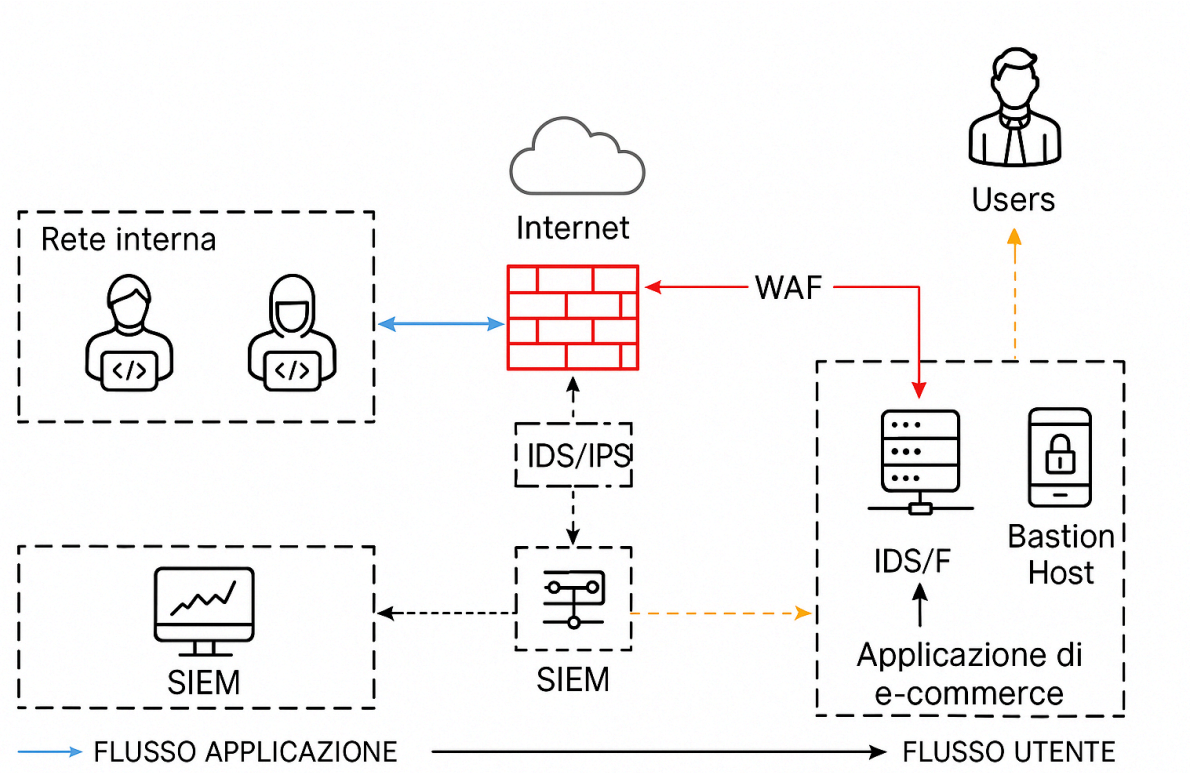
Mitigazione	Tool consigliato
CDN Anti-DDoS	Cloudflare, Akamai
Monitoraggio	Graylog, Wazuh, Splunk
SIEM	Wazuh, ELK Stack
SOAR (automatizzazione)	TheHive + Cortex, Shuffle

3. Risposta a infezione malware

Misura	Descrizione	Tool consigliato
Isolamento rete	Bloccare traffico dalla macchina infetta	VLAN + ACL
IDS/IPS	Rilevare attività sospette	Suricata, Snort
EDR	Identificare e contenere automaticamente	SentinelOne, CrowdStrike
Quarantine	Network Isolation dinamico	NAC, VLAN Switch
SIEM + SOAR	Automatizzare alert & containment	Wazuh + TheHive/Cortex

4. Soluzione integrata (infrastruttura sicura)

Architettura Sicura Proposta per la Web Application



Elementi architetturali consigliati:

- DMZ con firewall bidirezionali e ACL stretti
- WAF tra Internet e Web App
- IDS/IPS tra DMZ e rete interna
- EDR con regole automatiche di contenimento
- SIEM per centralizzazione dei log
- SOAR per orchestrare le risposte automatiche
- Backup cifrati su cloud privato/off-site

- Bastion Host come unico punto di accesso admin
- Zero Trust Architecture: accesso per identità e policy, non per posizione

---

5. Modifica aggressiva dell’infrastruttura (opzionale ma consigliata)

Componente	Aggiornamento
Segmentazione rete	Separare servizi front-end, back-end e DB
Accesso	Autenticazione MFA e bastion host
Architettura	Zero Trust: autenticazione continua, controllo per micro segmenti
Backup	Off-site, cifrato, monitorato da SIEM
Incident Response	Playbook testati e aggiornati (in stile MITRE)
Monitoraggio	Dashboard unificata su SIEM + alert automatici

Conclusione e prossimi step

L’architettura attuale espone rischi critici.
Con le misure proposte, l'infrastruttura potrà raggiungere un livello **intermedio-avanzato di sicurezza**, in linea con quanto previsto da ISO 27001, NIST CSF e MITRE.

Azioni consigliate a breve termine

- Installare WAF e IDS/IPS
- Configurare segmentazione della rete e controllo ACL
- Isolare DMZ e applicare policy Zero Trust
- Automatizzare il contenimento malware con EDR
- Implementare dashboard su SIEM + alert automatici