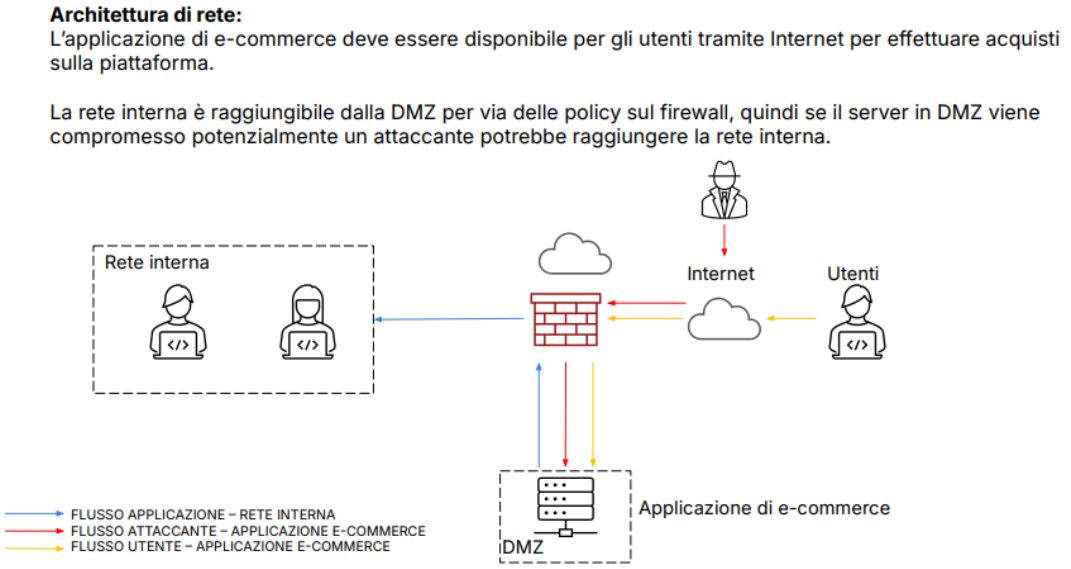
Report finale M5 - Security Operation

Salve Prof, questo report risponde in modo tecnico alle richieste della traccia, spiegando ogni termine tecnico, gli impatti sul business per far arrivare il contenuto ad un pubblico non tecnico.

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.



Richieste del progetto

Con riferimento all'architettura di rete, 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 vostra 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)

Azioni preventive

Quando si parla di sicurezza applicativa, soprattutto nel contesto di un'applicazione e-commerce esposta su Internet, SQL Injection (SQLi) e Cross-Site Scripting (XSS) rappresentano due delle minacce più comuni e pericolose. Entrambe le vulnerabilità derivano da una mancata validazione e sanificazione dell'input dell'utente, ed entrambe possono portare a compromissioni gravissime: furto di dati sensibili, accesso a dati interni, manipolazione delle transazioni o persino compromissione completa dell'infrastruttura.

Nell'immagine originale, vediamo che l'applicazione web si trova in DMZ (Demilitarized Zone) e comunica sia con l'utente finale che con la rete interna. Questo rappresenta un rischio: se un attaccante compromette la web application, può potenzialmente accedere anche alla rete interna.

PRINCIPALI AZIONI PREVENTIVE DA ADOTTARE

1. Implementazione di un WAF (Web Application Firewall)

   Un WAF è uno strumento che si interpone tra l'utente (o l'attaccante) e l'applicazione web. Ha il compito di analizzare il traffico HTTP in entrata e bloccare eventuali pattern riconducibili ad attacchi noti, come query SQL malevoli o script JavaScript iniettati. Un WAF ben configurato può prevenire in tempo reale exploit basati su SQLi o XSS.

2. Validazione e sanificazione dell'input lato server

   Ogni campo compilabile dell'utente deve essere validato lato server e sanificato. Utilizzare ORM, escapare i caratteri pericolosi e validare i dati ricevuti con modelli attesi permette di rendere inefficaci la maggior parte delle tecniche di injection.

3. Protezione tramite header di sicurezza http

   Intestazioni come Content-Security-Policy, X-XSS-Protection e X-Frame-Options difendono l'utente da script iniettati o attacchi clickjacking. È fondamentale configurare il web server per includere queste intestazioni in tutte le risposte HTTP.

4. Monitoraggio continuo tramite SIEM/SOAR

È importante monitorare il traffico alla ricerca di comportamenti anomali. Integrare log WAF, web server e database in un SIEM permette di rilevare proattivamente tentativi d'attacco. Con un SOAR è possibile anche bloccare automaticamente IP sospetti.

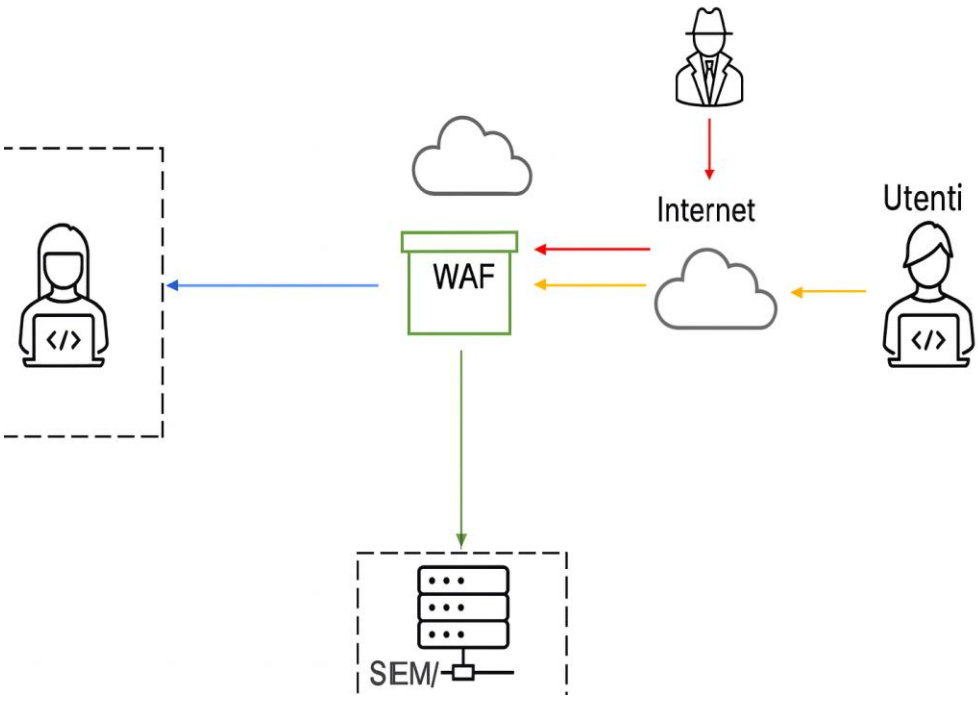
5. Scansioni periodiche con tool automatici

Software come OWASP ZAP, Nessus, OpenVAS consentono di identificare vulnerabilità note e mantenere un livello di sicurezza aggiornato. È consigliabile automatizzare le scansioni settimanali.

6. Aggiornamento costante della piattaforma

L'aggiornamento di CMS, librerie, framework e sistemi operativi riduce il rischio di exploit noti. È fondamentale monitorare i bollettini di sicurezza e applicare le patch tempestivamente.

Nell'immagine aggiornata, il WAF filtra il traffico in entrata verso l'applicazione, i log sono inviati al SIEM, e tutte le comunicazioni sono sotto controllo. Questo approccio garantisce una drastica riduzione del rischio SQLi/XSS.



Impatti sul business

Un attacco DDoS (Distributed Denial of Service) ha come obiettivo quello di rendere inaccessibile un servizio saturandolo con richieste massicce e simultanee provenienti da più fonti. Nel caso in esame, il downtime causato da tale attacco dura 10 minuti, durante i quali l'applicazione e-commerce non è disponibile per gli utenti.

Impatto sul business:

• Media di spesa al minuto sulla piattaforma: 1.500 €
• Durata dell'interruzione del servizio: 10 minuti
• Perdita economica diretta stimata: 1.500 € x 10 = 15.000 €

Questa perdita rappresenta solo l'impatto economico diretto. Tuttavia, un'interruzione del servizio può anche causare:

- Danno reputazionale: la fiducia degli utenti verso la piattaforma può diminuire sensibilmente, in particolare se l'attacco viene percepito come sintomo di scarsa sicurezza.
- Riduzione della fidelizzazione: clienti insoddisfatti potrebbero rivolgersi a competitor.
- Costi indiretti: aumentati tempi di supporto clienti, eventuali sconti offerti, SLA infranti.

Azioni preventive da adottare:

1. WAF con Rate Limiting

    Un Web Application Firewall configurato con regole di rate-limiting permette di identificare traffico anomalo e bloccare le richieste oltre una soglia accettabile. È una misura efficace per mitigare attacchi DDoS di livello applicativo.

2. Load Balancer e ridondanza infrastrutturale

    L'adozione di bilanciatori di carico e infrastrutture distribuite consente di diluire il traffico e mantenere operativo almeno parte del servizio anche in caso di attacco.

3. CDN (Content Delivery Network)

    Utilizzare una CDN permette di decentralizzare la distribuzione dei contenuti, rendendo più difficile saturare il server principale e migliorando i tempi di risposta anche sotto pressione.

4. Monitoraggio real-time con SIEM

    Avere un sistema SIEM permette di rilevare precocemente un attacco in corso, agendo con misure di contenimento automatizzate tramite l'integrazione con un SOAR.

5. Servizi anti-DDoS dedicati

    Provider come Cloudflare, AWS Shield, Akamai offrono protezione dedicata contro DDoS. Sono in grado di assorbire e mitigare grandi volumi di traffico malevolo.

Prevenire significa soprattutto garantire disponibilità continua, che nel modello CIA (Confidenzialità, Integrità, Disponibilità) è un pilastro fondamentale. Un investimento proattivo nella resilienza del sistema è sempre più economico di una reazione post-attacco.

Response

In caso di infezione da malware su un'applicazione web esposta su Internet, la priorità assoluta è impedire la propagazione del codice malevolo all'interno della rete aziendale. L'obiettivo in questo scenario non è rimuovere l'accesso da parte dell'attaccante, bensì isolare la macchina compromessa per contenere il danno.

La macchina infetta si trova all'interno della DMZ. Per evitare che il malware possa raggiungere i sistemi interni, è necessario agire a livello di rete. Questo implica modificare le policy firewall e implementare una rete di quarantena o una VLAN separata, escludendo qualsiasi canale di comunicazione tra la DMZ e la rete interna.

Isolando il server infetto:
- L'attaccante mantiene l'accesso, ma non può pivotare all'interno della rete.
- Il malware non può diffondersi verso altri asset o host critici.
- La situazione è sotto controllo mentre si avvia un processo forense e di remediation.

Azioni consigliate:

1. Isolamento tramite firewall:

    Bloccare tutto il traffico in uscita dal server infetto verso la rete interna. Questo include porte TCP/UDP, richieste HTTP, DNS e condivisioni SMB.

2. Segmentazione e quarantena:

    Spostare la macchina infetta su una rete separata (VLAN di isolamento) o configurare una regola di routing che la instradi verso una DMZ controllata con accesso limitato.

3. Monitoraggio e logging:

    Continuare a monitorare i log della macchina compromessa per raccogliere informazioni sull'attività dell'attaccante e sulle modalità di infezione.

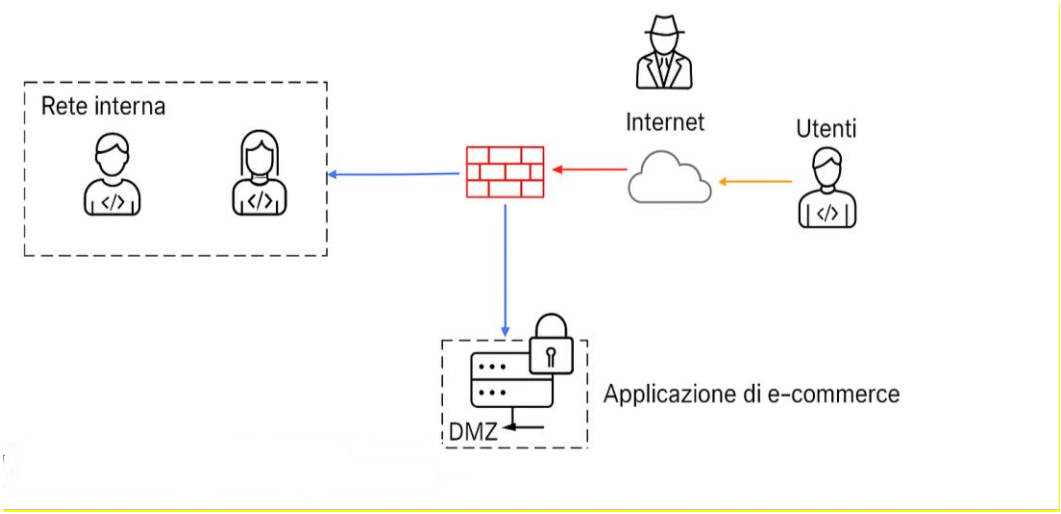
4. Aggiornamento degli antivirus aziendali:

    Blacklistare l'hash del malware nei motori antivirus e assicurarsi che tutti i dispositivi abbiano le firme aggiornate per evitare nuove infezioni.

5. Analisi forense:

    Effettuare un dump della macchina infetta, raccogliere indicatori di compromissione (IoC), e identificare il malware per analizzarne il comportamento.

Nell'immagine sottostante è mostrato il blocco della comunicazione tra la DMZ (dove si trova l'app infetta) e la rete interna. Il firewall impedisce qualsiasi traffico in uscita verso i server interni, mantenendo però aperta la comunicazione con Internet per fini investigativi e di contenimento controllato.



Soluzione completa

Questo capitolo ha lo scopo di integrare in un'unica strategia le due azioni fondamentali di sicurezza affrontate nei capitoli precedenti: le azioni preventive contro attacchi SQLi/XSS (Azioni preventive) e la risposta a una compromissione da malware (Response). L'obiettivo è costruire un'architettura resiliente sia in fase preventiva che in risposta agli incidenti.

Una strategia di sicurezza efficace non si limita all'adozione di misure singole, ma prevede una visione completa, capace di rilevare, prevenire, rispondere e contenere ogni tipo di minaccia informatica.

Elementi chiave della soluzione combinata:

1.Web Application Firewall (WAF):

Resta il primo livello di protezione esposto su Internet. Ha il compito di bloccare attacchi di tipo injection, XSS e altre minacce note prima che raggiungano l'applicazione. Deve essere configurato con regole aggiornate e specifiche per l'ambiente.

2. Logging centralizzato con SIEM:

Tutti gli eventi rilevanti provenienti da WAF, firewall, web server e host interni devono confluire in un sistema SIEM che permette il monitoraggio continuo e la correlazione tra eventi per rilevare comportamenti anomali.

3. Isolamento controllato della macchina infetta:

Nel caso in cui l'attacco vada a buon fine e un malware infetti la macchina in DMZ, è previsto un isolamento automatico. Il firewall blocca i flussi tra la DMZ e la rete interna ma mantiene il traffico con Internet per permettere il monitoraggio e l'analisi forense.

4. Aggiornamenti e scansioni regolari:

Il ciclo continuo di aggiornamento dei software e l'esecuzione programmata di vulnerability assessment prevengono la presenza di CVE sfruttabili da attori malevoli.

5. VLAN di quarantena:

Elemento fondamentale per contenere la propagazione del malware. Una VLAN isolata permette di gestire la macchina compromessa senza esporre gli altri asset aziendali.

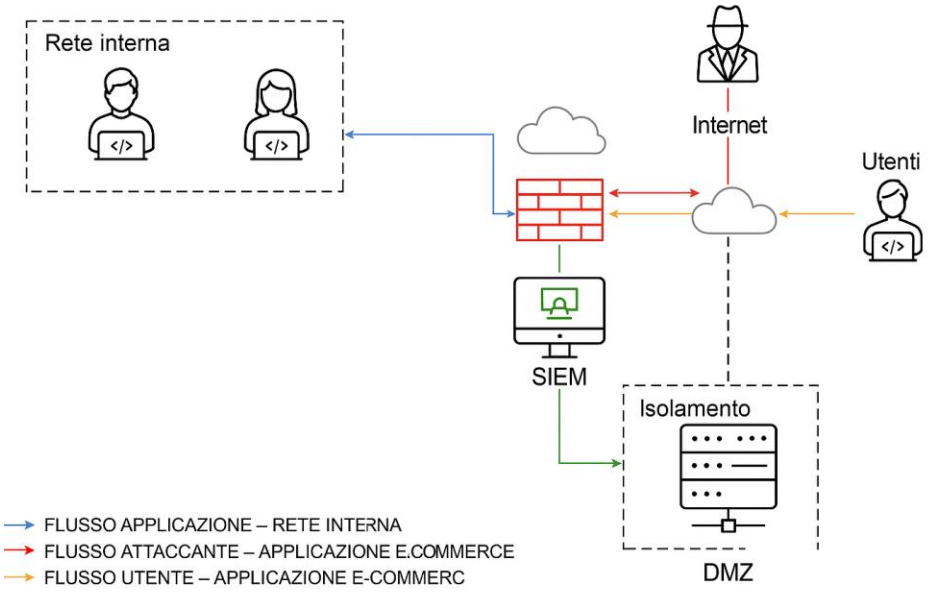
6. Flussi segmentati e controllati:

L'architettura complessiva prevede un controllo granulare dei flussi di rete: ogni segmento comunica solo con ciò che è strettamente necessario. Questo approccio Zero Trust riduce al minimo la superficie d'attacco.

L'unione delle misure preventive e delle soluzioni di contenimento costituisce una solida strategia di "defense-in-depth" che consente di resistere anche a compromissioni parziali, limitandone l'impatto e il raggio d'azione.

Segue una rappresentazione schematica della struttura aggiornata, integrando WAF, SIEM e l'isolamento del server infetto, per fornire un quadro visivo della difesa multilivello.

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



Modifica «più aggressiva» dell'infrastruttura

In questo ultimo capitolo analizziamo una modifica più aggressiva e strutturale all'infrastruttura, con un budget ipotetico compreso tra i 20.000 € e i 30.000 €. Lo scopo è innalzare ulteriormente il livello di sicurezza, continuità operativa e capacità di risposta, adottando soluzioni di tipo enterprise, professionale e proattivo.

Strumenti fondamentali consigliati:

1. Web Application Firewall avanzato (Cloudflare Business o AWS WAF):
- Protezione multi-layer con regole personalizzabili.
- Rate-limiting, captchas, e protezione bot inclusi.
- Costo stimato: 2.200 €/anno

2. SIEM/SOAR centralizzato (Microsoft Sentinel):
- Integrazione con Azure, log da server, endpoint, WAF, firewall.
- Automazioni tramite playbook di risposta (SOAR).
- Costo stimato: 5.200 €/anno per 100 utenti/device

3. Endpoint Detection and Response (Microsoft Defender for Endpoint P2):
- Protezione avanzata sugli host.
- Funzionalità EDR, antimalware, isolamento, forensic.
- Costo stimato: 5.100 €/anno per 100 dispositivi

4. Vulnerability scanning con OpenVAS:
- Software open-source con aggiornamento costante dei feed.
- Richiede un laptop dedicato (una tantum): 600 €

5. Server di backup e failover in cloud (AWS EC2 – T3 Medium):
- Avvio automatico in caso di compromissione o downtime.
- Costo stimato: ~230 €/anno

6. Segmentazione VLAN (Switch Cisco Catalyst):
- Separazione logica dei flussi.
- Rete per DMZ, interna, guest, quarantena, backup.
- Switch di fascia medio-alta: 1.500 € (una tantum)

7. Honeypot e trappole (Thinkst Canary):
- Server fittizi per attirare e tracciare i movimenti degli attaccanti.
- Licenza: 5.000 € + server dedicato 1.200 € (una tantum)

8. Formazione continua IT (LinkedIn Learning):
- Corso cybersecurity + SOAR + risposta agli incidenti.
- Licenza annuale per 5 dipendenti: 1.625 €

9. Nuovo firewall perimetrale (Fortinet 60F + licenza UTP):
- Maggiore throughput, filtraggio avanzato, VPN, IDS/IPS.
- Costo: 800 € + 700 € licenza UTP

Totale stimato: ~24.155 €

Raccomandazioni operative aggiuntive (senza costi diretti):

- Politiche Zero Trust per l'accesso dalla DMZ.
- Obbligo MFA e password manager aziendale.
- Disabilitare porte non necessarie (es. HTTP 80).
- Audit mensili di accesso privilegiato.

Questa configurazione avanzata trasforma la sicurezza da una reazione passiva a un sistema attivo di deterrenza, contenimento e risposta in tempo reale. Le spese sostenute si giustificano con la protezione degli asset digitali, la continuità del business e il rispetto delle normative di settore (es. GDPR, ISO 27001).

Conclusioni personali

Per quanto alta la sicurezza non è mai abbastanza in quanto, a parere mio non esiste un sistema sicuro, inteso come protetto al 100%. Questo lato del lavoro inoltre mi sembra anche fondamentale da sapere non solo per essere un tecnico Blue team ma anche per chi effettua Pentesting ed ethical hacking in quanto, sapendo cosa un difensore può vedere, cosa può implementare come sicurezza, di certo aiuta me “hacker” a prepararmi a dovere per eseguire correttamente il mio lavoro.