REPORT PROGETTO FINE MODULO W20D4

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?

Per prevenire eventuali danni all'infrastruttura e alla sicurezza dei dati aziendali, è fondamentale implementare una serie di azioni preventive, organizzate su più livelli. L'obiettivo principale è ridurre la superficie di attacco e rendere il più difficile possibile qualsiasi tentativo di accesso non autorizzato o di compromissione.

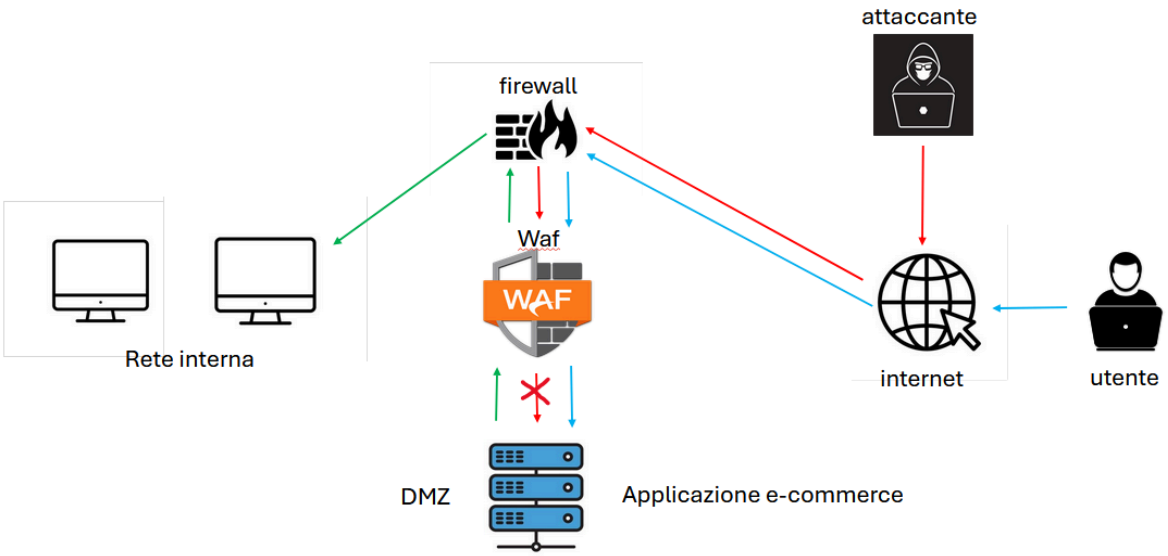
Come prima misura, abbiamo introdotto una **segmentazione della rete**, creando una **DMZ (zona demilitarizzata)**, che ospita i servizi accessibili pubblicamente, come il sito e-commerce. Questo permette di isolare la rete interna da attacchi esterni, anche nel caso in cui la parte pubblica venga compromessa. Nessun utente esterno può comunicare direttamente con il database o con i server interni: tutto passa attraverso firewall e sistemi controllati.

A livello **applicativo**, abbiamo previsto l'installazione di un **WAF – Web Application Firewall** – che agisce a livello 7 del modello **OSI**. Questo strumento filtra le richieste **HTTP** in ingresso e blocca automaticamente minacce comuni come **SQL Injection, XSS** e attacchi bot automatizzati. Il WAF è essenziale per proteggere applicazioni web esposte su Internet.

Per la definizione delle regole di sicurezza, ci siamo basati sulle linee guida proposte da **OWASP – Open Worldwide Application Security Project**. In particolare, il documento OWASP Top 10 ci ha aiutato a identificare le vulnerabilità più comuni, come l'SQL Injection e il Cross-Site Scripting (XSS), fornendo best practice per prevenirle già in fase di sviluppo. OWASP offre anche strumenti gratuiti come OWASP ZAP, uno scanner di vulnerabilità che consente di testare l'applicazione prima del rilascio in produzione.

Oltre il WAF, è importante aver migliorato anche la sicurezza dell'application web attraverso la sanitizzazione dell'input sia lato server che client.

Un altro punto fondamentale per prevenire eventuali attacchi è la **formazione del personale**, un sistema è sicuro solo quanto lo è l'anello più debole, spesso rappresentato dall'essere umano. Per questo motivo abbiamo incluso la formazione periodica del personale come azione preventiva chiave: riconoscere email di phishing, evitare comportamenti rischiosi, e utilizzare credenziali robuste è fondamentale per limitare i vettori di attacco non tecnici.



Il diagramma rappresenta un'architettura di rete progettata per proteggere un'applicazione web di e-commerce da attacchi esterni.
L'applicazione è ospitata all'interno di una **DMZ (zona demilitarizzata)**, separata dalla rete interna aziendale.

- **Gli utenti** legittimi accedono all'applicazione tramite Internet.
- **Il traffico** in ingresso è filtrato da un **WAF (Web Application Firewall)**, che blocca attacchi a livello applicativo come SQLi e XSS.
- Un **firewall perimetrale** gestisce le connessioni tra DMZ e rete interna, impedendo che attacchi o malware si propaghino verso i sistemi interni.
- Le **connessioni sospette** provenienti da un attaccante vengono bloccate già all'ingresso del WAF o del firewall, prevenendo danni all'infrastruttura aziendale.

Questa configurazione riduce la superficie d'attacco e isola le componenti più critiche del sistema.

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.

Un attacco **DDoS (Distributed Denial of Service)** ha colpito l'applicazione web, rendendola non raggiungibile per 10 minuti. Considerando che, in media, gli utenti spendono circa 1.500 € al minuto sulla piattaforma di e-commerce, la perdita economica diretta stimata è pari a **15.000 €**.

Oltre alla perdita economica immediata, si devono considerare anche danni indiretti, come la riduzione della fiducia dei clienti, il possibile abbandono del sito da parte degli utenti abituali e il danno reputazionale per l'azienda, soprattutto se gli episodi si ripetono.

Per ridurre l'impatto di attacchi come un **DDoS** e garantire la continuità operativa dell'azienda, è fondamentale affiancare alle contromisure tecniche anche **piani di gestione strutturati**, tra cui:

- **BCP (Business Continuity Plan)**: definisce come garantire la continuità dei servizi essenziali anche in caso di guasti o attacchi. Include piani di failover, replica geografica e uso di cloud resilienti.

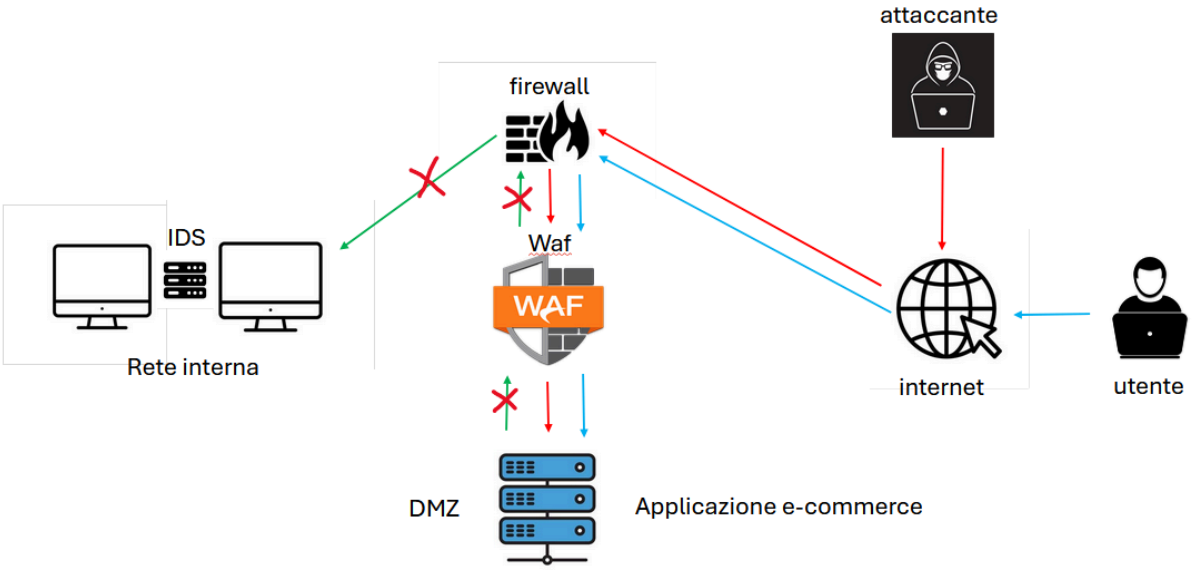
- **BIA (Business Impact Analysis)**: serve per identificare in anticipo le aree critiche del sistema e calcolare l'impatto economico e operativo in caso di fermo. In questo caso, il BIA evidenzierebbe la perdita di €15.000 per soli 10 minuti di inattività.

- **IRP (Incident Response Plan)**: è il piano operativo per reagire rapidamente a un attacco informatico. Include la procedura di contenimento, analisi dell'incidente, ripristino dei servizi e comunicazione interna/esterna.

Questi tre elementi sono fondamentali per assicurare una risposta efficace e minimizzare i danni sia economici che reputazionali. La sola difesa tecnica non basta: serve anche un approccio strategico e organizzato alla sicurezza.

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.

Nel caso in cui l'applicazione Web venga infettata da un malware, la nostra priorità principale è impedire che il malware si propaghi all'interno della rete aziendale, limitando così i danni potenziali e salvaguardando l'integrità degli altri sistemi e dati. Nonostante non sia nostro obiettivo immediato eliminare l'accesso dell'attaccante alla macchina infetta, il contenimento della minaccia deve essere rapido ed efficace.



Come si può notare nell'immagine, abbiamo applicato una misura di contenimento, in questo preciso caso, una rimozione completa della rete interna, per evitare ulteriormente la propagazione del malware. Pertanto la rete interna non ha accesso ad internet.

Questa è la misura più drastica possibile tra quelle di **contenimento**, ma è quella necessaria qualora bisogna prioritizzare l'integrità delle macchine critiche ed importanti.

Si può notare tra l'altro che così facendo l'attaccante mantiene l'accesso sulla **DMZ**, lasciando in balia del malware gli utenti dell'e-commerce. Evidentemente in questo caso l'azienda avrebbe valutato l'impatto di questo attacco e concluso che, a livello economico, sarebbe meglio "sacrificare" l'immagine (un'azienda che lascia in balia di un malware i propri utenti non è moralmente corretto) a favore di un danno economico-aziendale meno pronunciato. Ad esempio, l'azienda avrebbe potuto chiudere i battenti qualora il malware avesse infettato dei dispositivi di importanza critica e non ci fosse stato un backup valido per ripristinare i danni.

Nell’eventualità che il malware abbia già infettato un pc della rete interna, abbiamo un ulteriore “difesa” ovvero **IDS** e non **IPS** perchè in una fase così delicata **l'obiettivo non è bloccare automaticamente il traffico, ma monitorare e analizzare con precisione il comportamento del malware** all'interno della rete isolata.

Un IPS potrebbe generare **falsi positivi** e compromettere la disponibilità di servizi interni fondamentali o interrompere comunicazioni legittime, aggravando la situazione. In questo scenario, dove è già in atto un attacco e la priorità è l’**analisi forense e il contenimento passivo**, l'IDS ci consente di:

- Rilevare eventuali **movimenti laterali** del malware;
- Tracciare tentativi di connessione verso altri host interni;
- Studiare **i pattern di attacco** e i payload senza interferire direttamente con il traffico;
- Preparare una risposta mirata, basata su evidenze raccolte.

In pratica, l’IDS viene posizionato tra i segmenti di rete interna, ad esempio tra la **VLAN** dei server interni e quella dei client, così da fungere da “osservatore” silenzioso capace di rilevare segnali di compromissione senza alterare l’equilibrio operativo.

Questa configurazione è coerente con la decisione strategica di **non rimuovere immediatamente l’accesso dell’attaccante**, ma di raccogliere il massimo numero di informazioni utili prima di un’eventuale operazione di rimozione o bonifica.

Infine, tutto il traffico viene registrato e inviato a un **SIEM (Security Information and Event Management)** per l’analisi centralizzata, utile a rafforzare le difese future e integrare l’incidente nel piano **IRP (Incident Response Plan).**

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

Piano di Investimento per la Sicurezza Informatica – Budget 25.000 €

Supponiamo che la nostra azienda, composta da 50 dipendenti, abbia a disposizione un budget di 25.000 € da investire in soluzioni di sicurezza informatica. Di seguito sono elencate le principali aree di intervento selezionate, con relativi costi e motivazioni.

1. Protezione DDoS + WAF - (Cloudflare Business)

Una protezione efficace contro gli attacchi DDoS è imprescindibile. Per questo motivo abbiamo scelto il servizio **Cloudflare Business**, che offre difesa contro attacchi di livello L3, L4 e L7 (es. TCP/UDP Flood, HTTP Flood), oltre a includere un **Web Application Firewall (WAF)**.

- **Costo:** 200 €/mese → **2.400 €/anno**

2. Formazione del Personale - (Piano Diamond di KnowBe4)

Per aumentare la consapevolezza interna e ridurre il rischio umano (phishing, errori di configurazione, ecc.), abbiamo incluso un piano di formazione continua.

- Costo medio stimato: **3 €/mese per dipendente**
- Per 50 dipendenti → **1.650 €/anno**

3. Firewall di nuova generazione (NGFW)

Abbiamo scelto **Fortinet FortiGate 60F**, un firewall di nuova generazione che include:
IPS, prevenzione malware basata su AI, filtraggio DNS/URL/video, controllo applicazioni, antispam e altro.

- **Durata licenza:** 3 anni
- **Costo totale (hardware + licenza): 2.290 €**

4. IDS nella rete interna

Per migliorare la visibilità e il monitoraggio del traffico interno, è stato installato **Suricata**, un IDS open-source, su un mini-PC dedicato con **pfSense**.

- **Software:** gratuito
- **Costo hardware stimato: 500 €**

5. Backup automatici – (Veeam + Wasabi)

La combinazione di **Veeam** (gestione backup) e **Wasabi** (cloud storage) garantisce la sicurezza e la disponibilità dei dati aziendali in caso di guasto o attacco ransomware.

- **Veeam:** 7 €/mese per utente → **4.200 €/anno**
- **Wasabi:** 6,99 $/TB al mese, stimando 10 TB → **~840 €/anno**
- **Totale backup annuale: 5.040 €**

6. Replica applicativa - (VPS DR) (OVHCloud)

Per aumentare la resilienza, è prevista una copia dell'applicazione web principale su una VPS secondaria (Disaster Recovery) presso **OVHCloud**, attivabile manualmente in caso di disastro.

- **Durata offerta:** 2 anni
- **Costo totale: 2.400 €**

7. Penetration Test Web Application

Per identificare vulnerabilità nella nostra applicazione e-commerce, abbiamo previsto un penetration test completo. Il costo può variare tra 3.000 € e 10.000 €, ma si stima un investimento medio di:

- **Pen Test stimato: 5.000 €**

Totale spese: 19.280€

Fondi rimasti per eventuali spese extra o danni aziendali improvvisi: 5.718€