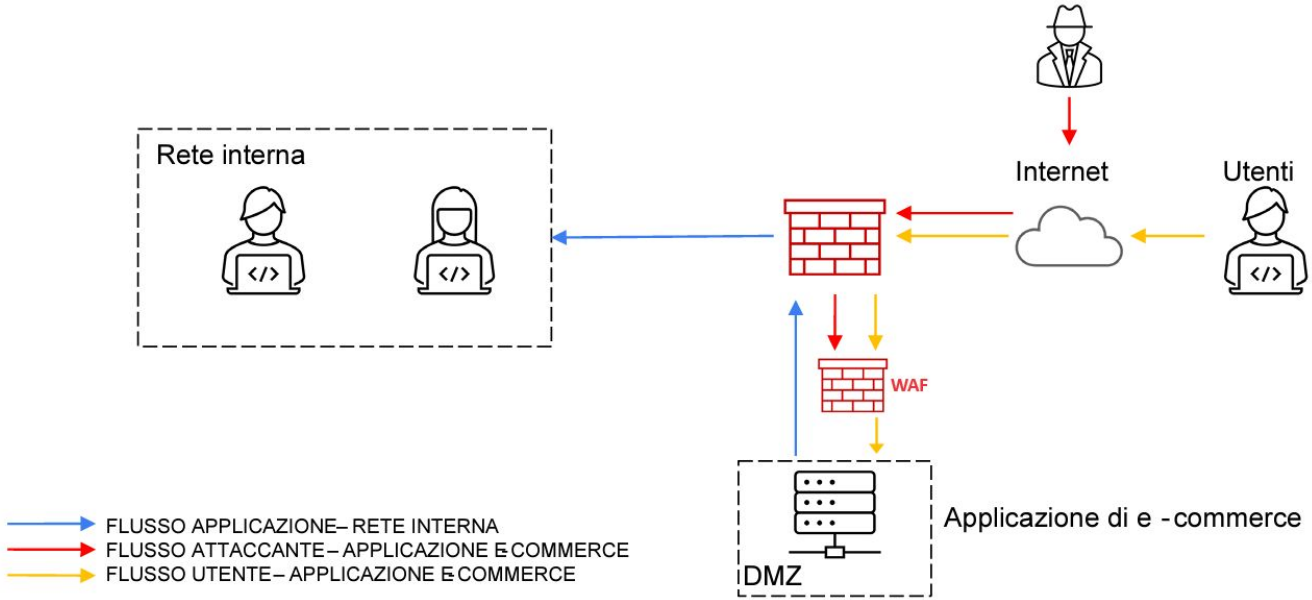
# Progetto S9/L5

# Azioni preventive

**Traccia:** Quali azioni preventive implementereste 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.

Per la protezione della Web App da minacce quali XSS e SQLi, è possibile adottare preventivamente una soluzione basata su Web Application Firewall (WAF). Questi, a differenza dei firewall standard, sono progettati specificamente per proteggere le Web App da attacchi XSS e SQLi. La figura iniziale si modifica di conseguenza, considerando che il WAF protegge il traffico in entrata sulla Web App proveniente da Internet (quindi utenti e attaccanti).

# Azioni preventive



# Impatti sul business

**Traccia:** 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.

L'attacco di tipo DDoS causa l'inaccessibilità della piattaforma di e-commerce per 10 minuti. Considerando che gli utenti spendono circa 1.500€ al minuto, possiamo stimare i danni causati dal mancato guadagno sul business moltiplicando la spesa potenziale degli utenti per minuto (1.500€) per i minuti di indisponibilità del servizio (10).

**Impatto sul business = 1.500 € x 10 minuti = 15.000 €**

Quindi, per 10 minuti di indisponibilità, la compagnia ha perso 15.000 € di acquisti potenziali. Le azioni preventive sono elencate nella prossima slide.

# Impatti sul business

**Servizio di Mitigazione DDoS per Applicazioni Web:**

- Considera l'utilizzo di servizi specifici di mitigazione DDoS progettati per proteggere contro gli attacchi che mirano alle vulnerabilità delle applicazioni web.

**Bilanciamento del Carico Applicativo:**

- Implementa il bilanciamento del carico a livello di applicazione per distribuire il traffico tra più server, garantendo che l'applicazione web possa gestire un volume più elevato di richieste.

**Cache e CDN per Contenuti Statici:**

- Utilizza servizi di caching e Content Delivery Network (CDN), come ad esempio Cloudfare, per distribuire contenuti statici. Questi servizi possono ridurre il carico sui tuoi server principali e proteggere l'applicazione dalle congestioni causate dagli attacchi DDoS.

**Pianificazione di Backup e Recupero:**

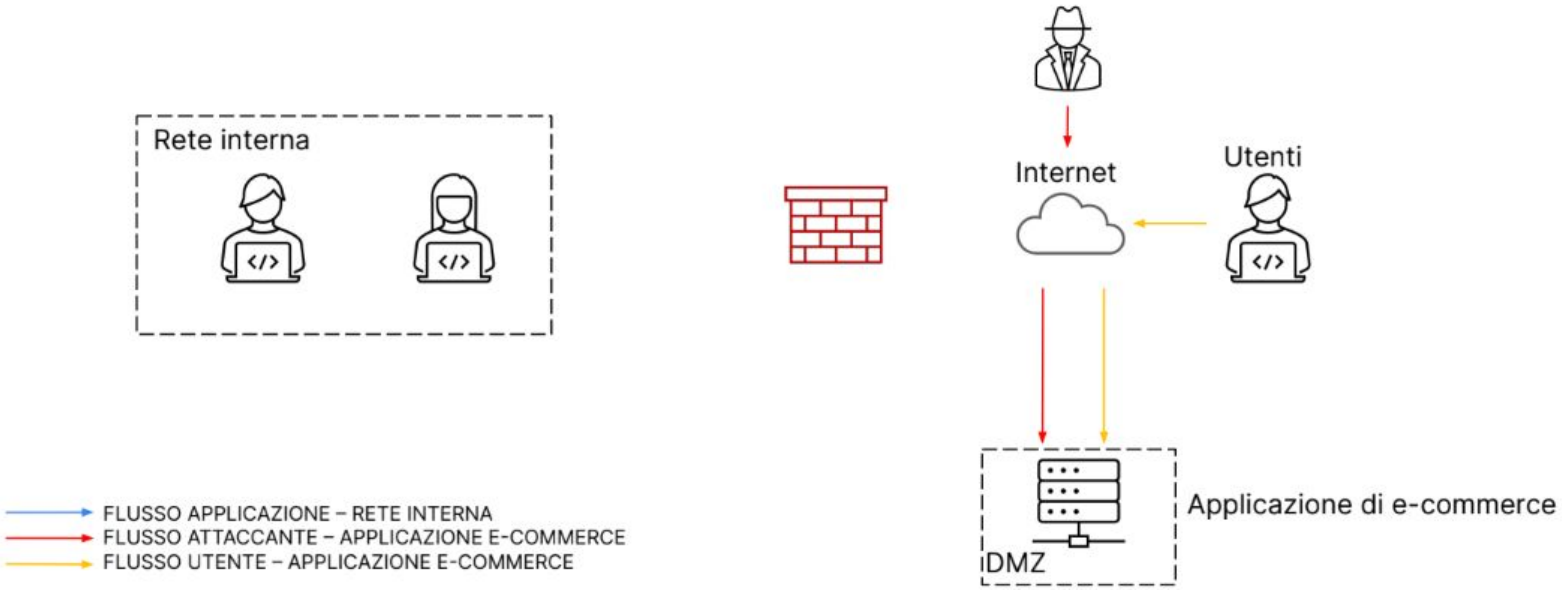
- Crea piani di backup e recupero per garantire che tu possa ripristinare rapidamente l'applicazione in caso di interruzione del servizio dovuta a un attacco DDoS.

# Response

**Traccia:** 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.

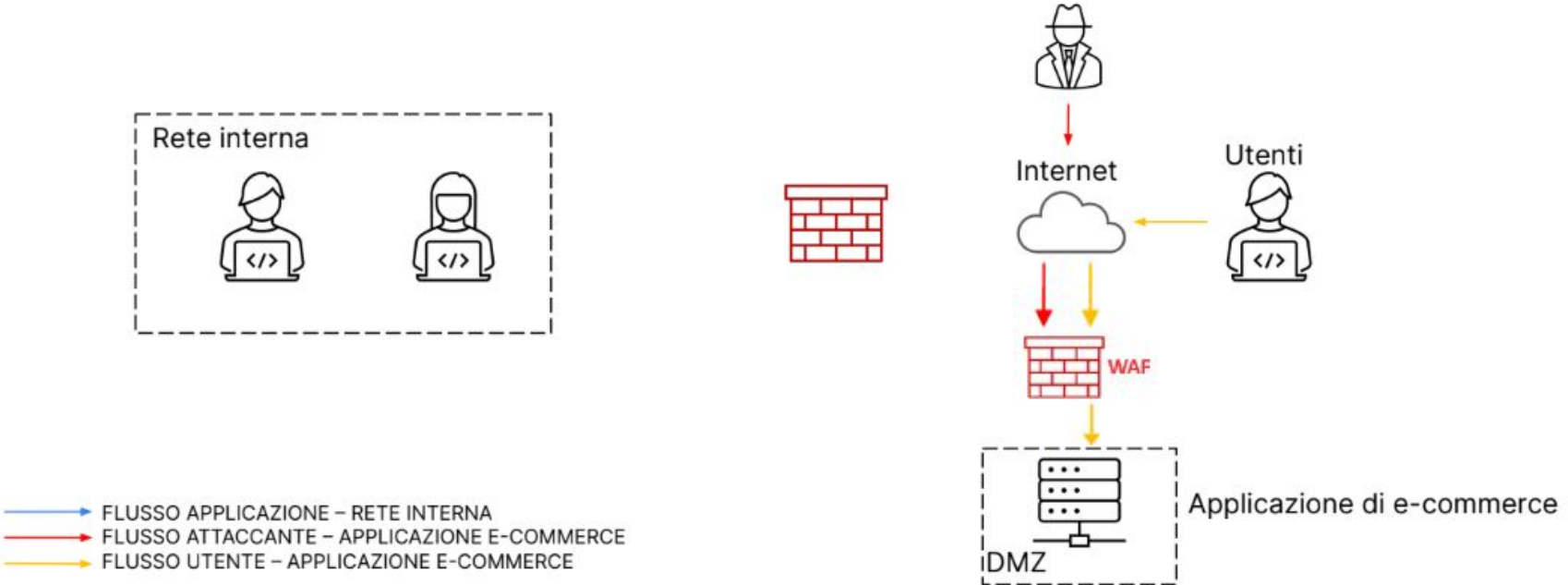
Considerando la priorità, si può adottare una strategia basata sull'isolamento della macchina infettata. In questo caso, la macchina sarà direttamente collegata a Internet, quindi accessibile dall'attaccante, ma non sarà più connessa alla rete interna. La figura nella prossima slide mostra la soluzione con la strategia dell'isolamento della macchina infetta, evidenziando come non ci sia più comunicazione tra l'applicazione web e la rete interna.

# Response


Rete interna
Internet
Utenti
DMZ
Applicazione di e-commerce
FLUSSO APPLICAZIONE – RETE INTERNA
FLUSSO ATTACCANTE – APPLICAZIONE E-COMMERCE
FLUSSO UTENTE – APPLICAZIONE E-COMMERCE

# Soluzione completa

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



# Modifica «più aggressiva» dell'infrastruttura

**Traccia**: Integrando eventuali altri elementi di sicurezza (se necessario/facoltativo magari integrando la soluzione al punto 2).

Ecco le mie considerazioni con un budget modesto (circa 7000€):

**Sistemi di Rilevamento e Risposta agli Incidenti (IDS/IPS):**

- L'implementazione di IDS/IPS può aiutare a rilevare comportamenti sospetti nella rete e bloccare o mitigare automaticamente gli attacchi.

**Monitoraggio Avanzato del Traffico di Rete:**

- Utilizzare strumenti di monitoraggio avanzato per analizzare il traffico di rete in tempo reale, identificando anomalie e attività sospette

# Modifica «più aggressiva» dell'infrastruttura

**Distribuzione su Più Server e Bilanciamento del Carico:**

- Distribuire l'applicazione su più server può ridurre il rischio di un singolo punto di fallimento. L'utilizzo di servizi di bilanciamento del carico contribuisce a distribuire uniformemente il traffico tra i server, migliorando la resistenza e la disponibilità del servizio.

**Aggiornamenti Regolari e Patching:**

- Assicurarsi di mantenere tutti i componenti del sistema e del software aggiornati regolarmente per coprire le vulnerabilità note.

**Formazione e Consapevolezza degli Utenti:**

- Implementare programmi di formazione per gli utenti e i manager per aumentare la consapevolezza sulla sicurezza informatica e ridurre il rischio di attacchi basati sull'ingegneria sociale.

# Bonus

**Traccia:** Analizzare le seguenti segnalazioni caricate su anyrune fare un piccolo report di ciò che si scopre relativo alla segnalazione dell'eventuale attacco spiegando ad utenti e dirigenti la tipologia di attacco e come evitare questi attacchi in futuro:
https://app.any.run/tasks/8e6ad6d9-4d54-48e8-ad95-bfb67d47f1d7/

https://app.any.run/tasks/60b9570f-175b-4b03-816b-a38cc2b0255e/

# Bonus: Primo Link

La task coinvolgeva l'esecuzione di un file denominato "PERFORMANCE_BOOSTER_v3.6.exe", situato nella cartella temporanea dell'utente. Questo file ha generato due processi figlio, uno dei quali ha eseguito un file batch, mentre l'altro ha eseguito un comando PowerShell per modificare la policy di esecuzione. La task includeva anche la creazione di un file di backup del registro e la modifica di chiavi di registro relative a PowerShell e alle impostazioni Internet. Inoltre, sono state apportate modifiche a diversi file nella cartella temporanea dell'utente. Gli eventi più significativi di questa task includono l'esecuzione di un file batch e di un comando PowerShell per cambiare la policy di esecuzione. Ciò suggerisce un tentativo di aggirare le misure di sicurezza per abilitare l'esecuzione di script potenzialmente dannosi. La creazione di un file di backup del registro e la modifica delle chiavi di registro relative a PowerShell e alle impostazioni Internet indicano altresì tentativi di modificare le configurazioni di sistema a fini malevoli. La modifica dei file nella cartella temporanea dell'utente potrebbe indicare la presenza di ulteriori file o script dannosi. In conclusione, questa task coinvolgeva l'esecuzione di un file dalla cartella temporanea dell'utente, generando processi figlio e eseguendo varie azioni come la modifica di chiavi di registro e file. I punti più interessanti includono i tentativi di cambiare la policy di esecuzione e di modificare le chiavi di registro, indicando un'attività potenzialmente dannosa. Si consiglia un'ulteriore analisi per identificare eventuali file o script dannosi aggiuntivi e comprendere appieno l'estensione dell'impatto della task.

# Bonus: Secondo Link

La task ha coinvolto l'utilizzo di Edge ed è iniziata con l'esecuzione di "MicrosoftSetup.exe", seguita da "MicrosoftUpdate" e "MicrosoftUpdate.exe". Questi erano probabilmente utilizzati per l'aggiornamento di Microsoft Edge. La task ha comportato la modifica di chiavi di registro correlate a Edge e EdgeUpdateState. L'evento più interessante in questa task è la modifica delle chiavi per l'aggiornamento di EdgeClient. Ciò indica che la task stava eseguendo un processo di aggiornamento relativo a Microsoft Edge.

Un altro evento rilevante è la creazione di file nella cartella temporanea. Questi file sono collegati all'aggiornamento e contengono informazioni importanti a riguardo.

In conclusione, questa task è centrata sull'aggiornamento di Microsoft Edge, coinvolgendo modifiche nel registro e la creazione di file temporanei. Le azioni svolte sono tipiche di un processo di aggiornamento e contengono informazioni cruciali per ulteriori analisi.

# Bonus

Per evitare simili attacchi in futuro, è possibile adottare diverse misure di sicurezza e buone pratiche. Ecco alcune raccomandazioni:

**1. Consapevolezza e Formazione:**

**Sensibilizzazione degli Utenti:** Fornire formazione regolare agli utenti per renderli consapevoli delle minacce potenziali, come l'apertura di file sospetti provenienti da fonti non attendibili

**2. Controllo degli Eseguibili:**

**Whitelisting:** Configurare una lista bianca (whitelist) di applicazioni approvate per l'esecuzione, limitando così l'accesso a eseguibili non autorizzati.

**3. Monitoraggio del Traffico di Rete:**

**Analisi del Traffico:** Utilizzare soluzioni di monitoraggio del traffico di rete per individuare modelli anomali o attività sospette, specialmente durante il trasferimento di file o l'esecuzione di comandi PowerShell.

# Bonus

**4. Controllo degli Accessi e delle Autorizzazioni:**

**Limitare i Privilegi:** Assegnare privilegi minimi necessari agli utenti e alle applicazioni, riducendo così le possibilità di esecuzione di comandi dannosi.

**5. Protezione del Registro di Sistema:**

**Controllo delle Modifiche al Registro:** Monitorare e controllare le modifiche al registro di sistema per individuare attività sospette o non autorizzate.

**6. Filtraggio del Contenuto Web:**

**Filtrare Contenuti Dannosi:** Utilizzare filtri web per bloccare l'accesso a siti web noti per distribuire malware o contenuti dannosi.

# Bonus

**7. Politiche di Sicurezza PowerShell:**

**Limitare l'Esecuzione di Script:** Configurare politiche di sicurezza PowerShell per limitare l'esecuzione di script solo da fonti attendibili e firmati digitalmente.

**8. Gestione delle Patch**:

**Mantenere Aggiornati i Sistemi:** Assicurarsi che il sistema operativo e le applicazioni siano sempre aggiornati con le ultime patch di sicurezza.

# Bonus

**9. Soluzioni Antimalware:**

**Software Antivirus/Antimalware:** Utilizzare soluzioni antivirus/antimalware aggiornate per rilevare e bloccare attività malevole.

**10. Analisi Forense:**

**Analisi Post-Attacco:** Dopo un possibile attacco, condurre un'analisi forense per identificare la portata dell'incidente e adottare misure correttive.

Implementare una combinazione di queste misure può contribuire significativamente a rafforzare la sicurezza del sistema e prevenire attacchi simili in futuro.