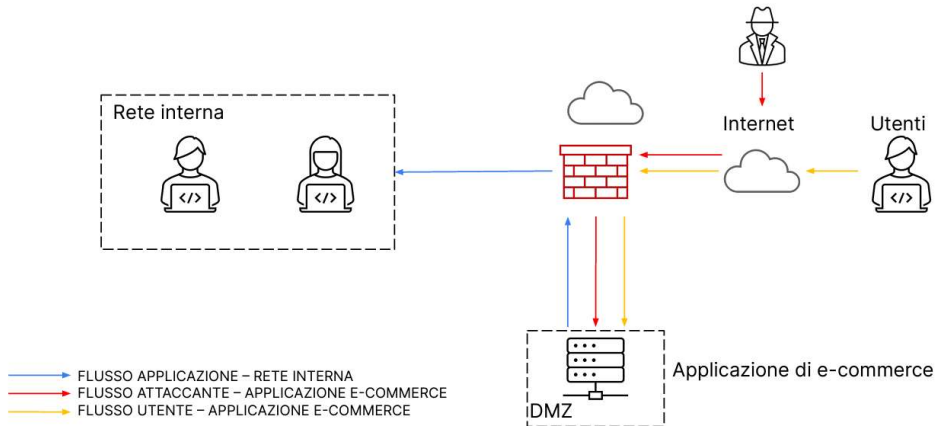
Traccia

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
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 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.
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 2)

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.



1. Azioni Preventive

Prima di affrontare specificamente le azioni preventive per difendere un'applicazione web da attacchi di tipo SQL injection (SQLi) e cross-site scripting (XSS), è importante comprendere l'importanza di seguire le best practice di incident response (Ad es: CSIR-Procurement-Guide-1). Queste best practice sono fondamentali per la gestione efficace delle minacce alla sicurezza informatica e includono una serie di procedure e azioni preventive per proteggere un'organizzazione dalle potenziali violazioni della sicurezza. Tra queste, troviamo:

- Vulnerability Assessment
- Penetration Test
- Threat Analysis

Inoltre, è cruciale riconoscere che la sicurezza informatica è un processo continuo e multifase. Oltre a seguire le best practice di incident response, è essenziale implementare soluzioni di sicurezza aggiuntive per ridurre il rischio di attacchi informatici e proteggere le risorse critiche dell'organizzazione. Queste soluzioni svolgono un ruolo chiave nella difesa proattiva contro le minacce informatiche e tra queste troviamo:

- Network Access Control (NAC)
- Next Generation Firewall (NGFW)
- Web Application Firewall (WAF)
- Security Information and Event Management (SIEM)
- Secure Development Lifecycle (SDLC)
- Aggiornamento regolare del software

1.1. Vulnerability Assessment:

- Utilizzare strumenti di vulnerability scanning per identificare e correggere vulnerabilità note nell'applicazione web e nel server sottostante.
- Scansionare regolarmente l'applicazione e il codice sorgente per individuare potenziali falle di sicurezza, tra cui vulnerabilità SQLi e XSS.
- Implementare controlli di validazione e sanitizzazione dei dati di input per prevenire l'inserimento di stringhe dannose o script nei campi dei moduli web.

1.2. Penetration Test:

- Condurre penetration test per valutare l'efficacia delle misure di sicurezza implementate e identificare eventuali falle di sicurezza che potrebbero essere sfruttate da attaccanti.
- Simulare attacchi di tipo SQL injection e XSS durante il penetration test per valutare la resistenza dell'applicazione agli attacchi e identificare eventuali vulnerabilità non rilevate dal vulnerability assessment.
- Testare le contromisure di sicurezza, come filtri input e meccanismi di validazione, per garantire che siano adeguatamente configurate e funzionanti.

1.3. Threat Analysis:

- Condurre un'analisi delle minacce per identificare potenziali vettori di attacco e valutare il livello di rischio associato.
- Prioritizzare le azioni preventive in base alla gravità potenziale dell'impatto e al grado di esposizione al rischio.
- Implementare l'utilizzo di piattaforme di Threat Intelligence per ottenere informazioni in tempo reale sulle minacce note e potenziali vettori di attacco.

1.4. Network Access Control (NAC):

- Il Network Access Control (NAC) è una tecnologia che gestisce e controlla l'accesso alla rete, garantendo che solo dispositivi autorizzati e conformi alle politiche di sicurezza abbiano accesso alla rete.
- Implementando un NAC, è possibile prevenire l'accesso di dispositivi non autorizzati o compromessi alla rete, riducendo il rischio di exploit e attacchi provenienti dall'interno della rete.

1.5. Next-Generation Firewall (NGFW):

- Il Next-Generation Firewall (NGFW) offre funzionalità avanzate di protezione da minacce, integrando firewall tradizionale con caratteristiche avanzate come Intrusion Prevention System (**IPS**), Intrusion Detection System (**IDS**).
    - **IPS:** è un sistema di sicurezza di rete che analizza il traffico di rete in tempo reale e blocca le attività dannose, utilizza una varietà di tecniche per identificare le attività dannose, tra cui:
        - Firma del pacchetto: confronta i pacchetti di rete con una
        - lista di firme note di attacchi.
        - Ispezione del payload: analizza il contenuto dei pacchetti di rete per cercare codice dannoso.
        - Analisi del comportamento: monitora il comportamento della rete per identificare modelli anomali che potrebbero indicare un attacco.
    - **IDS:** è un sistema di sicurezza di rete che analizza il traffico di rete in tempo reale e identifica le attività dannose.
        - Gli IDS non bloccano le attività dannose, ma inviano avvisi agli amministratori di rete in modo che possano prendere le opportune misure.
        - Gli IDS utilizzano le stesse tecniche degli IPS per identificare le attività dannose.

- Un NGFW può rilevare e mitigare attacchi SQLi e XSS, fornendo un controllo granulare sul traffico di rete e applicativo per identificare e bloccare in tempo reale le minacce.
- Effettua analisi su tutti in livelli della pila ISO/OSI fino al livello 7

1.6. Web Application Firewall (WAF):

- Implementare un WAF per filtrare il traffico HTTP/HTTPS in ingresso all'applicazione web e bloccare automaticamente attacchi SQLi e XSS.
- Configurare regole personalizzate per identificare e mitigare specifici tipi di attacchi e monitorare il traffico sospetto.

1.7. Security Information and Event Management (SIEM):

- Integrare un SIEM per il monitoraggio costante del traffico di rete e degli eventi di sicurezza.
- Raccogliere, correlare e analizzare i dati provenienti da diversi dispositivi e sistemi di sicurezza per individuare e rispondere prontamente a eventuali anomalie o attività sospette.

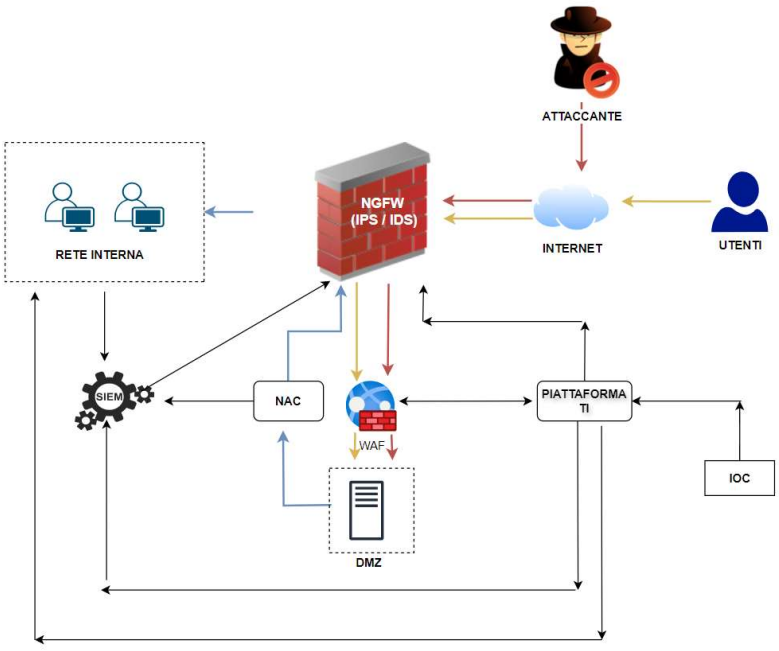
1.8. Secure Development Lifecycle (SDLC):

- Implementare il SDLC, un approccio strutturato per integrare la sicurezza nel processo di sviluppo del software fin dalle prime fasi del ciclo di vita del prodotto.
- Identificare e mitigare le vulnerabilità fin dall'inizio dello sviluppo dell'applicazione web, riducendo il rischio di esposizione a futuri attacchi.

1.9. Aggiornamento regolare del software:

- Assicurarsi che tutti i software utilizzati nell'ecommerce (come piattaforme CMS, framework, plugin, librerie) siano aggiornati regolarmente con le ultime patch di sicurezza.

1.10. Nuova Architettura di rete



2. Impatti sul Business

2.1. Calcolo impatto finanziario

- **Importo medio speso ogni minuto:** 1.500 €
- **Durata dell'attacco DDoS**: 10 minuti
- **Impatto finanziario totale dell'attacco DDoS =** Importo medio per minuto * Durata dell'attacco = 1.500 €/min * 10 min = **15.000 €**

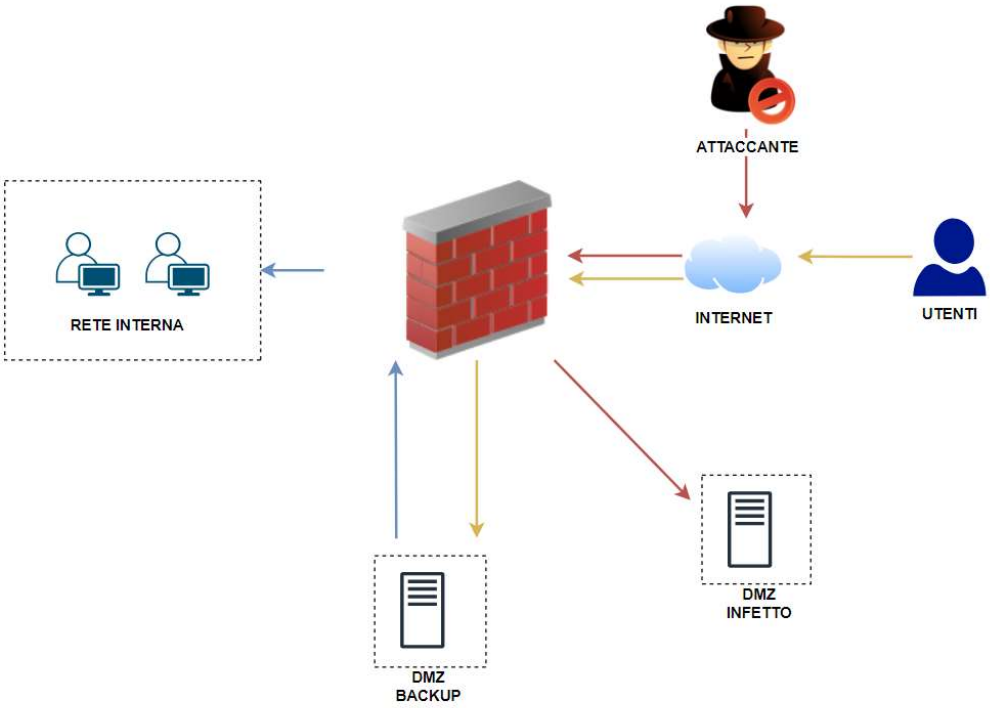
Quindi, l'impatto finanziario dell'attacco DDoS sulla piattaforma di e-commerce è di 15.000 €.

2.2. Azioni Preventive

Per prevenire tali interruzioni future, potrebbe essere necessario implementare una soluzione di mitigazione DDoS, come un servizio di protezione anti-DDoS. Questo tipo di servizio è progettato per rilevare e mitigare gli attacchi DDoS in tempo reale, riducendo l'impatto del downtime sulla piattaforma di e-commerce. Tuttavia, è importante valutare attentamente i costi associati a questa soluzione preventiva e assicurarsi che siano proporzionati al valore del business e ai potenziali danni finanziari causati dagli attacchi DDoS. Se il costo della protezione anti-DDoS supera l'impatto finanziario previsto del DDoS, potrebbe essere necessario esplorare alternative o soluzioni più economiche oppure decidere un'accettazione del rischio in base alla mole di attacchi subiti.

3. Response

3.1. Nuova Architettura di rete



3.2. Soluzione

Per garantire la Business Continuity e proteggere l'integrità della nostra rete, adotteremo misure di isolamento per limitare la diffusione del malware e mitigare gli effetti degli attacchi informatici. L'isolamento è una pratica di sicurezza che coinvolge la separazione di sistemi o reti compromessi o potenzialmente compromessi dal resto dell'infrastruttura IT.

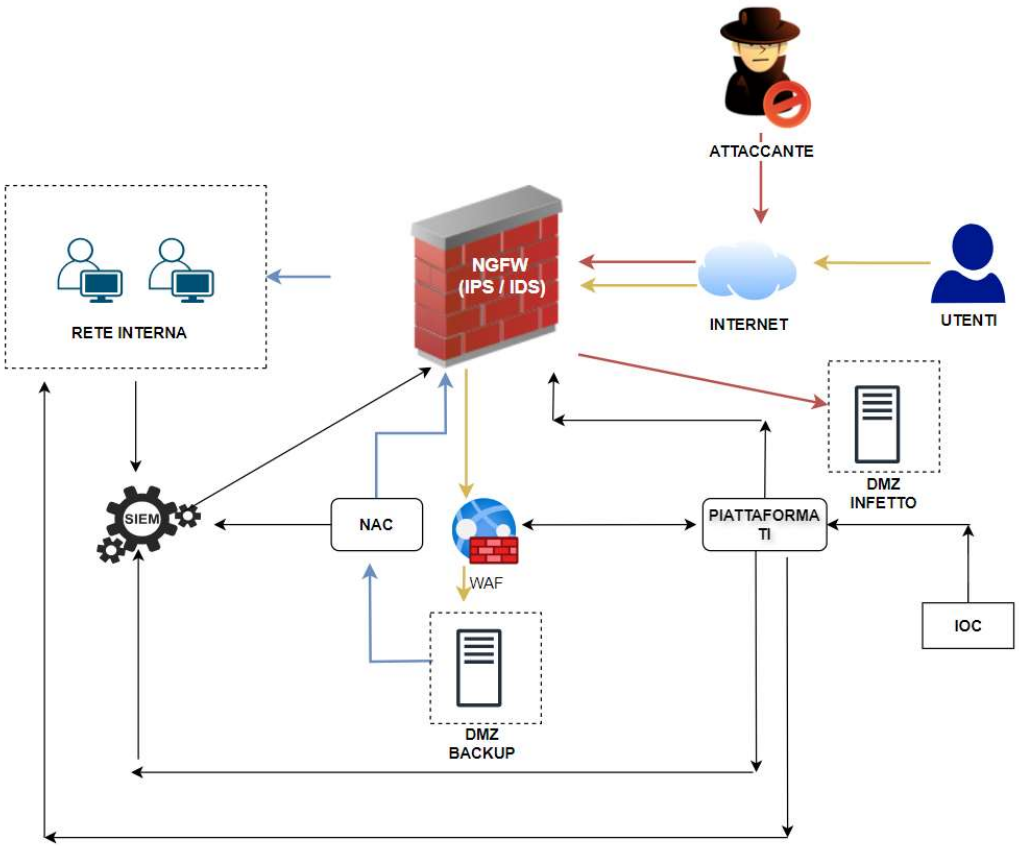
Nel nostro contesto, ciò significa attivare una DMZ di backup e isolare la DMZ infetta, impedendo al malware di diffondersi all'interno della nostra rete aziendale. La DMZ di backup sarà pronta a sostituire la DMZ principale, garantendo la continuità operativa e riducendo al minimo l'impatto degli attacchi.

Isolare la DMZ infetta comporta la disconnessione o la limitazione delle comunicazioni tra la DMZ compromessa e il resto della rete aziendale. Questo impedisce al malware di propagarsi ulteriormente e limita i danni causati agli altri sistemi e alle risorse della rete.

Allo stesso tempo, lasceremo attiva la connettività Internet sulla DMZ infetta in modo da condurre un'analisi comportamentale sull'attaccante e identificare nuove vulnerabilità che potrebbe sfruttare. Questo ci permetterà di studiare il comportamento dell'attaccante in tempo reale, raccogliere informazioni sulle tattiche e le tecniche utilizzate e sviluppare contromisure adeguate per mitigare il rischio di futuri attacchi.

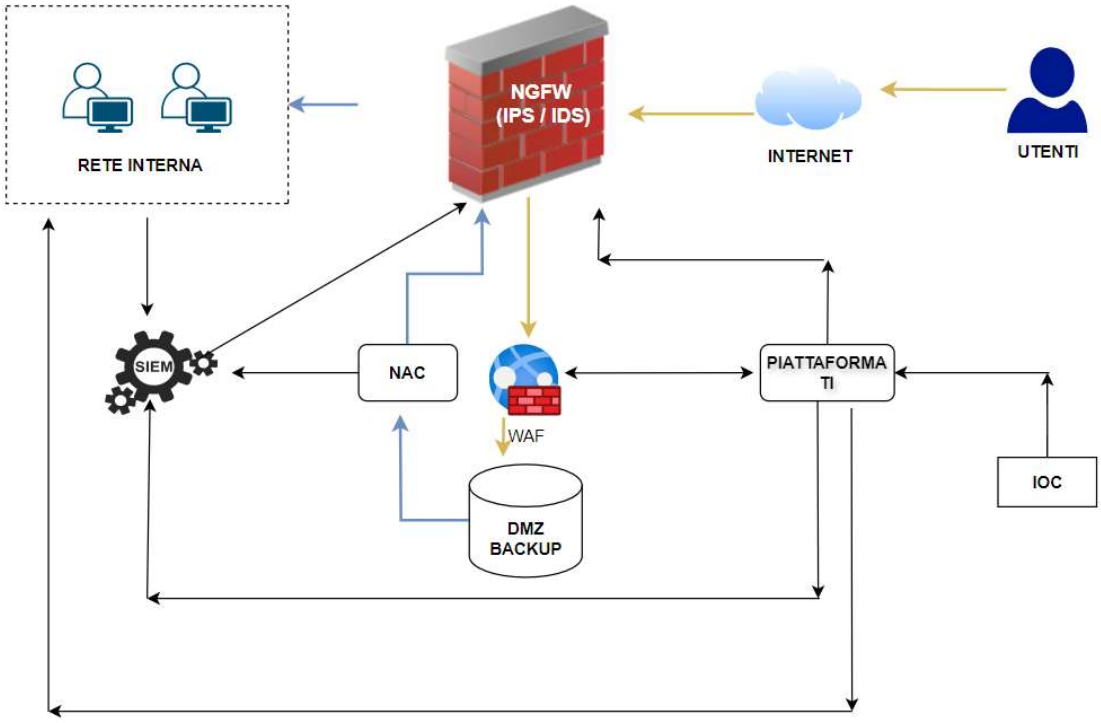
4. Soluzione Completa

4.1. Nuova Architettura di rete



5. Modifica Aggressiva

5.1. Nuova Archiviazione di rete



5.2. Soluzione

Rimozione della DMZ infetta: Questo può coinvolgere la disconnessione dei cavi di rete, la disabilitazione delle porte di rete sui dispositivi di rete o la rimozione delle configurazioni che permettono la comunicazione con la DMZ infetta.
Dopo aver rimosso la DMZ infetta dalla rete, è essenziale procedere con la pulizia del server che ospitava la web app infetta dal malware. In questo contesto, abbiamo a disposizione tre opzioni per la pulizia del server:

- **Clear:** il dispositivo viene completamente ripulito dal suo contenuto con tecniche «logiche». Si utilizza ad esempio un approccio di tipo read and write dove il contenuto viene sovrascritto più e più volte o si utilizza la funzione di «factory reset» per riportare il dispositivo nello stato iniziale.

- **Purge:** si adotta non solo un approccio logico per la rimozione dei contenuti sensibili, come visto nel caso di clear, ma anche tecniche di rimozione fisica come l'utilizzo di forti magneti per rendere le informazioni inaccessibili su determinati dispositivi

- **Destroy:** è l'approccio più netto per lo smaltimento di dispositivi contenenti dati sensibili. Oltre ai meccanismi logici e fisici appena visti, si utilizzano tecniche di laboratorio come disintegrazione, polverizzazione dei media ad alte temperature, trapanazione. Questo metodo è sicuramente il più efficace per rendere le informazioni inaccessibili ma è anche quello che comporta un effort in termini economici maggiore.