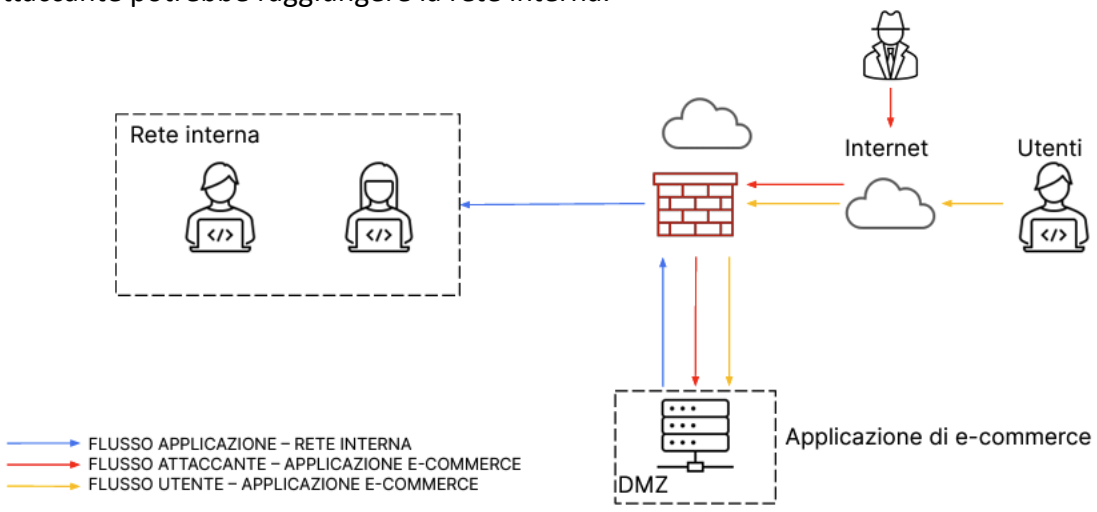
# Modulo 5 Progetto - Russo Alessio

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 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 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 venisse compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.




**Tenendo in considerazione la seguente figura:**

Si possono definire delle azioni preventive, ossia quelle azioni che servono a prevenire i rischi di eventi negativi, response per l'incident e azioni post incident intese come quelle misure che mirano a correggere e rafforzare la sicurezza informatica.

1. **Azioni preventive attacchi di tipo SQLi o XSS:**

In caso di attacco SQLi o XSS si possono prevedere misure sia tecniche che procedurali.
Ad esempio, alcune di queste azioni potrebbero essere:

- **Filtrare le connessioni** in ingresso in modo da identificare e neutralizzare eventuali utenti malevoli effettuando controlli network
    - Il Filtraggio in questi casi può essere effettuato:
        - direttamente sulle WEB App attraverso un WAF (Web Application Firewall)
        - Sull' intera rete aggiungendo misure di sicurezza come:
            - NAC (Network Access Control)
            - Firewall
            - **IPS / IDS**: i sistemi di prevenzione e rilevamento delle intrusioni servono ad individuare preventivamente potenziali attacchi alle reti ed alle macchine in modo da bloccare eventuali utenti con comportamenti sospetti come immagine in basso

- **Controlli sui software** al fine di individuare bug nei software di gestione dei DB:
    - Sanificazione del codice in modo tale da identificare eventuali caratteri speciali che consentono ad u attaccate di effettuare un SQL injection (Alcuni processi possono essere: Validazione Input e Analisi statica del codice)
    - Reverse Engineering per accedere al codice sorgente in modo da limitare eventuali XSS (Alcuni processi possono essere: Analisi del codice Sorgente e Test di sicurezza dell'Applicazione WEB)

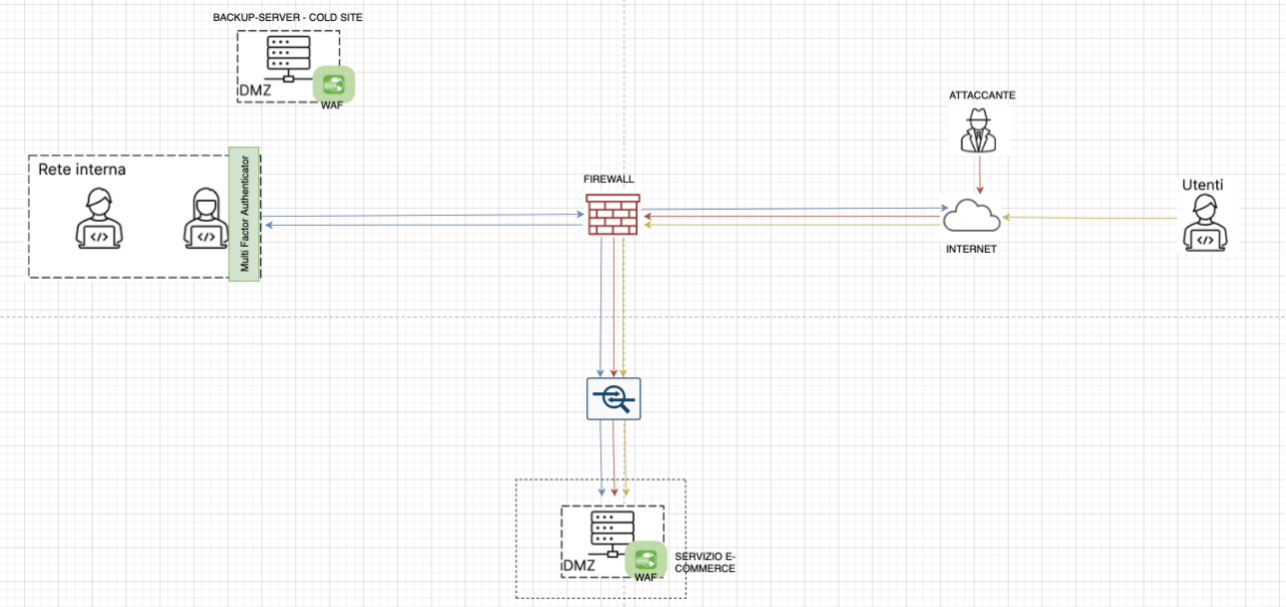
- **Controllo sui server** contenente il DB dell'e-commerce attraverso individuazione e correzione di eventuali bug (hardening, patch, GPO) o effettuando dei penetration testing sulleweb app in modo da individuare eventuali vulnerabilità note o zero-day effettuando test periodici.

- **Back Up dei Dati** in modo da non perdere informazioni in caso di incidente e riprendere agevolmente le attività relative almeno al core aziendale. Questa pratica non solo consente di ripristinare le informazioni cruciali, ma riduce anche il rischio di interruzioni prolungate delle attività aziendali che nel caso di un e-commerce potrebbero portare ad ingenti perdite in termini monetario (quantitative) e di immagine/reputazionali (qualitative). In questo caso l'azienda ricorre al metodo di back Up Cold-site ossia un ambiente non in uso attivamente ma che viene attivato solo in caso di emergenza

- **MFA (Multi Factor Authenticator)**: in modo da preservare l'identità delle persone che effettuano accesso ai sistemi aziendali effettuando una doppia verifica in fase di Login. L'implementazione di un sistema MFA rappresenta un importante strato aggiuntivo di sicurezza per preservare l'identità degli utenti che accedono ai sistemi aziendali. Aggiungere meccanismi di autenticazione di questo tipo per accedere alle risorse aziendali come, ad esempio, server o database dell'e-commerce potrebbe essere un buon livello di sicurezza da implementare all'interno del perimetro aziendale.

**Immagine riassuntiva** dei processi di implementazione dei controlli e di filtraggio citati in precedenza dove si nota che:
Al netto dei processi descritti sopra a livello grafico si nota che:

- È stato aggiunto l'utilizzo di un WAF (Web Application Firewall) direttamente sulle WEB App presente sul Server
- Sono state implementate misure di sicurezza a livello di rete come Firewall, IPS/IDS (Figura blu tra server e Firewall).
- Viene considerata la possibilità di effettuare backup (Cold Site - viene attivato in caso di necessità) dei dati per ridurre il rischio di perdita di informazioni cruciali in caso di incidenti e per riprendere rapidamente le attività online.
- Utilizzo di MFA (Multi Factor Authenticator) per una doppia verifica durante il login, preservando l'identità degli utenti e aggiungendo un livello di sicurezza aggiuntivo nell'accesso alle risorse aziendali.




2. **Impatti sul Business:** Considerando un attacco DDOS che rende l'applicazione non raggiungibile per 10 minuti e che in media gli utenti al minuto spendono 1500 € possiamo calcolare secondo i principi di BIA. Per calcolare l'impatto sul business possiamo:

   Calcolo SLE (Single Loss Expectancy):

   SLE = Importo speso dagli utenti al minuto * Minuti di non raggiungibilità del servizio

   SLE = €1500 * 10 minuti = €15,000

   Calcolo dell'ARO (Annualized Rate of Occurrence):

   L'ARO per un attacco DDoS dipende da vari fattori, uno ad esempio potrebbe essere l'attrattiva della piattaforma di e-commerce per gli attaccanti.

Una stima potrebbe essere, ad esempio, un attacco DDoS ogni 6 mesi.

ARO = 1 evento ogni 6 mesi = 0.5 eventi all'anno

Calcolo dell'ALE (Annualized Loss Expectancy):

ALE = SLE * ARO

ALE = €15,000 * 0.5 = €7,500

Quindi, l'ALE previsto dovuto alla non raggiungibilità del servizio a causa di un attacco DDoS è di 7,500 € all'anno.

**Azioni preventive:**

- **Implementazione di un sistema di mitigazione DDoS per rilevare e mitigare gli attacchi DDoS in tempo reale, come ad esempio servizi CloudFlare**

  In questo caso, considerando la perdita di 7500€ e un costo del servizio mensile di 200€ la soluzione da implementare servizi CloudFlare sembra conveniente in quanto il Delta sarebbe positivo per:

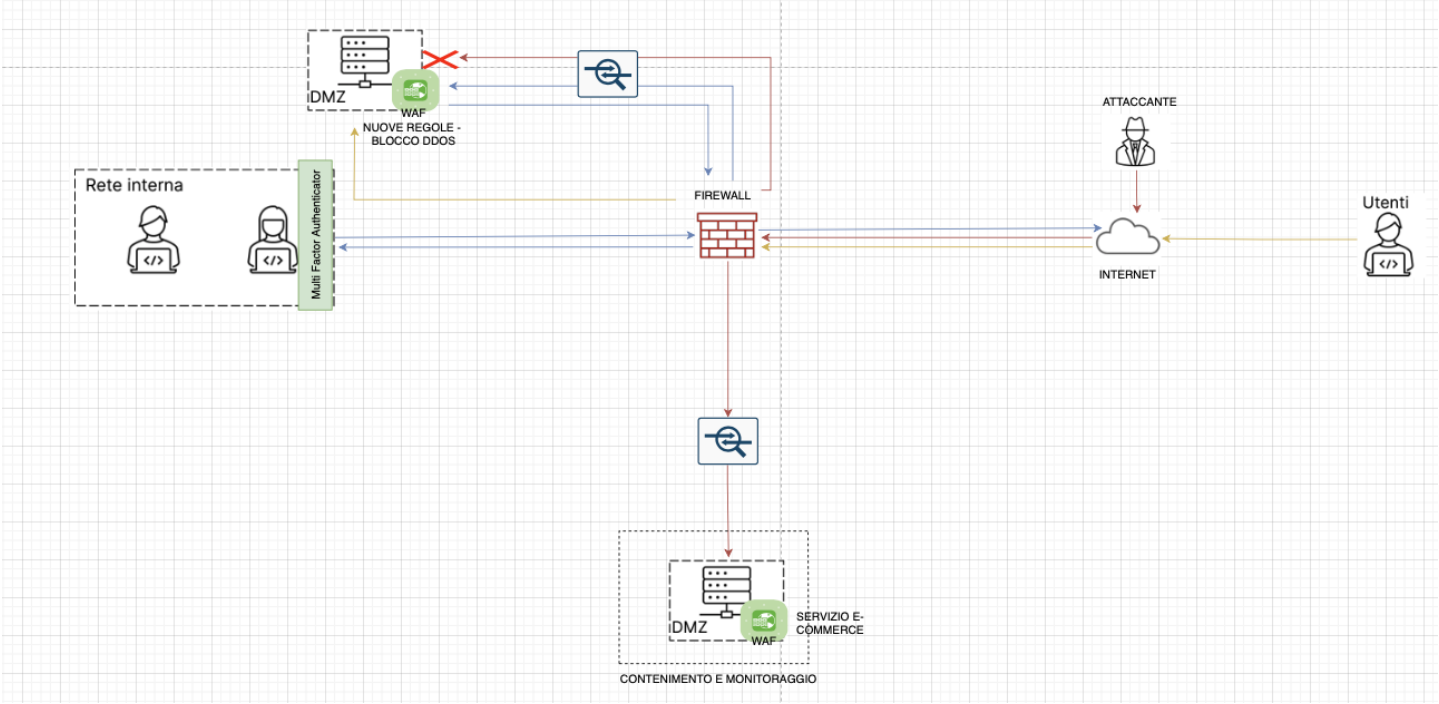
  ALE= 7500€
  Costo del Servizio Annuo = 200* 12 = 2400€
  Beneficio di Implementazione = 7500 - 2400 = 5100 €

  Considerando quanto detto in precedenza il Ritorno dell'investimento di sicurezza o ROSI sarà:

  ROSI = [(ALE - Costo del servizio Annuo) / Costo del Servizio Annuo] * 100
  ROSI = [7500 - 2400) /2400] * 100
  ROSI = 112,5 %
  Quindi possiamo introdurre i servizi CloudFlare per aumentare le soluzioni di Sicurezza in quanto l'impatto sarà estremamente positivo

3. **Response:** In caso di attacco DDoS (Distributed Denial of Service) contro un e-commerce, è fondamentale agire rapidamente e in modo efficace per mitigare gli effetti dannosi dell'attacco e ripristinare la disponibilità del sito web.
   In risposta all'attacco, il punto principale è impedire la propagazione del malware sulla rete isolando il server infetto, questo può essere fatto attraverso l'implementazione di misure di sicurezza come firewall per bloccare il traffico dannoso inoltre è utile disconnettere il server infetto dalla rete principale.
   Non rimuovere immediatamente l'accesso dell'attaccante al server è utile a monitorare attentamente le attività dell'attaccante per comprendere meglio l'entità e le motivazioni dell'attacco nonché può aiutare nella formulazione di strategie di difesa più efficaci e nel

raccogliere prove per eventuali azioni legali. Parallelamente, si identificano e correggono le vulnerabilità dell'asset che hanno permesso l'infezione.




L'immagine di cui sopra comprende anche la soluzione del punto 5

Punto 5: **Per rafforzare le attività di sicurezza informatica si potrebbe pensare di effettuare una modifica più aggressiva della struttura. Quindi si potrebbe:**

- Implementare la presenza di un **SOC** (ipotizzando un e-commerce di grandi dimensioni che internalizza le attività di monitoring aumentando i costi di gestione). Il SOC tiene sotto controllo tutto il perimetro aziendale che comprende: Firewall, IPS/IDS, WAF, Rete interna (endpoint) e Server)

- **Monitoraggio dei log** attraverso l'implementazione di un insieme di tool che vengono racchiuse in un SIEM per individuare a rispondere prontamente alle minacce di sicurezza nei software di gestione dei DB o più in generale in caso di attacchi su qualsiasi tipo di asset relativo ad un'azienda. Il monitoraggio dei log dell'applicazione web è un processo che coinvolge la registrazione e l'analisi delle attività e degli eventi che si verificano all'interno dell'applicazione web stessa. L'obiettivo principale del monitoraggio dei log è rilevare e rispondere tempestivamente a eventuali minacce alla sicurezza informatica, identificando comportamenti sospetti o attacchi in corso. Questo aiuta a garantire la protezione dei dati sensibili, la prevenzione di violazioni della sicurezza e la continuità delle operazioni nell'ambiente dell'applicazione web.

- **Attività di Threat Intelligence** utili a comprendere le minacce Cyber, identificare potenziali attaccanti e adottare misure di sicurezza prontamente. Categorie di TI sono:
  - **Strategic intelligence**
  - **Tactical intelligence**
  - **Operational intelligence**

Utili rispettivamente a fornire informazioni sulle minacce e potenziali attori malevoli (Strategic), fornire dettagli tecnici utili a rispondere prontamente alle minacce (Tactical), Fornire dettagli per prevenire le minacce (Operational).

- **Utilizzo di sonde di monitoraggio del traffico di rete** per rilevare segnali precoci di un possibile attacco DDoS e attivare misure preventive in anticipo. Le sonde possono essere posizionate all'interno della rete per monitorare il traffico e identificare comportamenti sospetti che potrebbero indicare un attacco in corso.

- **Implementazione di regole firewall più robuste e aggiornate** (frutto delle informazioni e dell'esperienza acquisite dal precedente attacco) per bloccare il traffico dannoso proveniente da indirizzi IP sospetti o noti per essere associati ad attacchi DDoS.

- **Formazione dei dipendenti** per prevenire o rispondere prontamente a successive minacce a livello sistemico/aziendale.