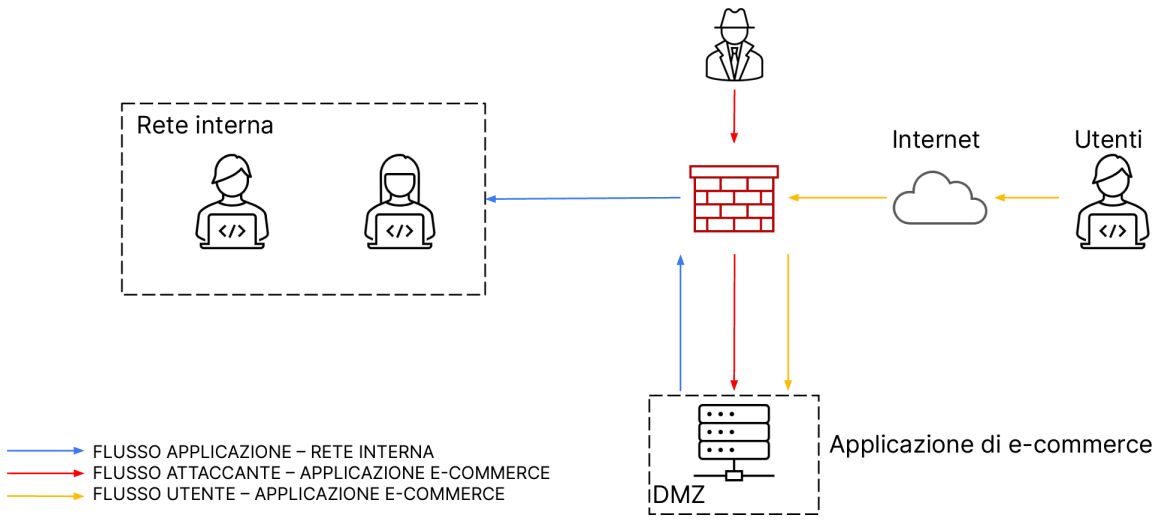
PROGETTO S9-L5

INDICE

1. Traccia

Con riferimento alla figura, rispondere ai seguenti quesiti.
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.
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.
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 con la soluzione proposta.

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.



2. Riferimenti teorici

La **sicurezza di un ambiente informatico** viene parametrata sulla base di «principi fondamentali». Uno dei principi cardine e più importanti per valutare lo stato della sicurezza delle informazioni di un dato ambiente è il «**CIA principle**», dove:

- C, sta per Confidentiality, ovvero la riservatezza del dato;
- I, sta per Integrity, ovvero l'integrità del dato;
- A, sta per Availability, ovvero la disponibilità del dato.

Generalmente, i controlli di sicurezza sono valutati in base al loro impatto sulle componenti del «CIA principle» (detto anche CIA triade).

RISERVATEZZA DEL DATO -> l'accesso al dato, che deve essere garantito solamente agli utenti autorizzati:
cifratura e le tecniche di controllo degli accessi.

INTEGRITA' DEL DATO -> proteggere l'affidabilità e la correttezza del dato e prevenire modifiche non autorizzate al dato:
meccanismi di controllo accessi ed autenticazione oltre a meccanismi di verifica degli hash, o checksum.
L'integrità del dato dipende dalla riservatezza del dato.

LA DISPONIBILITA' DEL DATO -> deve essere garantita in ogni momento e per i soli utenti autorizzati ad accedere alla risorsa in oggetto:
meccanismi di anti-denial of service, backup, ridondanza dell'infrastruttura, e tutte quelle altre misure di sicurezza che garantiscono la disponibilità dei servizi/dati in situazioni di criticità.

Riduzione del rischio: introducendo delle «security **remediation** action», ovvero delle azioni di rimedio per ridurre/eliminare il rischio.
Accettazione del rischio: accettando il rischio residuo.
Rimozione del rischio: rimuovendo l'asset (laddove non critica) soggetta al rischio.

Il **Security Operation Center (SOC)** è un sotto-dipartimento all'interno del dipartimento di Sicurezza che eroga servizi finalizzati alla protezione dei sistemi informatici, quali:

- **Servizi di gestione e manutenzione dell'infrastruttura IT** delle compagnie, come ad esempio, la manutenzione dei server, degli switch di rete, degli applicativi.
- **Servizi di monitoraggio e risposta** con lo scopo di individuare tempestivamente eventuali «minacce» (anche chiamate «**security threats**») ed in caso di attacco andato a buon fine, ha il compito di rispondere prontamente per limitare i danni. Al fine di settare gli strumenti e le configurazioni, è importante capire da quali tipi di minacce bisogna difendersi. Questa fase prende il nome di «**threat identification**». Minacce «avversarie»; Minacce «strutturali o infrastrutturali»; Minacce «ambientali»; Minacce «accidentali».
- **Rafforzamento della protezione dell'infrastruttura IT** con servizi proattivi come i Vulnerability Assessment o i Penetration test.

Un «**incidente di sicurezza**» si riferisce ad un evento che ha un impatto negativo sulla riservatezza, integrità o disponibilità di una data risorsa, come risultato di un attacco esterno oppure di un azione volutamente dannosa proveniente dall'interno e si includono anche gli eventi ambientali e accidentali (incidente). Ci sono **Azioni preventive** o **Azioni correttive e di risposta** agli incidenti.

Minaccie Cyber
Botnets: sono reti di computer dove un'entità centrale, che prende il nome di control-and-command server (CC server), invia istruzioni a una rete distribuita di computer, che prendono il nome di Zombie, precedentemente infettati tramite virus/malware. Lo scopo di una botnet è effettuare attacchi simultanei contro target in maniera centralizzata, causando impatti negativi sulla disponibilità dei servizi.
Denial-of-service (DoS): gli attacchi DoS hanno lo scopo di mettere fuori uso un servizio in esecuzione su un sistema, come potrebbe essere un'applicazione web o un sito web. Una delle forme più comune di attacco DoS è la trasmissione di un numero ingente di pacchetti ad un server al fine di saturare la CPU, dove si intende che la CPU è al 100% di utilizzo e non può di conseguenza processare altre richieste. La forma più comune di DoS è il **Distributed DoS (DDos)**, ovvero un attacco di tipo denial-of-service che viene inviato contemporaneamente verso un target da sorgenti multiple.

Azioni preventive
Le azioni preventive possono essere viste come l'insieme dei controlli di sicurezza che vengono adottati da una compagnia per aumentare il livello di **protezione perimetrale ed interna** al fine di ridurre il rischio di potenziali attacchi.

CONTROLLI NETWORK
- **NAC:** network access control.
- **Firewall:** Packet filtering firewall, Stateful inspection firewall, Next Generation Firewall (NGFW), Web Application Firewall.
- **Segmentazione di rete:** DMZ, ovvero l'area della rete che espone i servizi accessibili da internet, Internal Network, ovvero l'area delle rete che ospita i server che erogano i servizi accessibili dall'interno.
- **IPS / IDS:** i sistemi di prevenzione e rilevamento intrusioni servono ad individuare preventivamente potenziali attacchi alle reti ed alle macchine.

CONTROLLI SUGLI END-POINT (quali laptop, personal computer, smartphone o server)
- Hardening dei sistemi e delle configurazioni
- Patching dei sistemi
- Group policy
- Penetration testing

CONTROLLI SUL SOFTWARE (il software fa parte dell'asset della compagnia)
- Code analysis: statica o dinamica.
- Reverse engineering

LOGGING E MONITORING
È quell'insieme di procedure e tecniche che permettono di tracciare tutte le azioni su un determinato sistema da parte degli utenti, come ad esempio il login, il logout, la modifica delle impostazioni ed altri eventi significativi.
Logging: le applicazioni, i servizi, i sistemi e gli altri asset infrastrutturali generano «log» di default, o hanno la possibilità di farlo se correttamente configurati. I «log» sono dei file contenenti gli eventi e le attività che si verificano su un dato sistema, che includono altri dati quali: la data e l'ora in cui l'evento si è verificato, l'utente che ha eseguito l'azione ed il sistema sul quale si è verificato l'evento. Log di sicurezza; Log di sistema; Log applicativi; Log dei Firewall -> spesso vengono inviati ad un sistema centralizzato chiamato **SIEM – Security information event management** («log collector»), che ha il compito di correlare le informazioni provenienti da diverse sorgenti ed automatizzare il monitoraggio.
Monitoring: si introduce il concetto di «accountability», ovvero di «responsabilità». Per aumentare i livelli di automatismo, spesso si implementano delle policy di sicurezza che in presenza di determinati eventi anomali fanno scattare degli «alert di sicurezza».
Nonostante le misure di sicurezza messe in atto, alcuni eventi esterni possono impattare negativamente sulla sicurezza delle compagnie, come può essere un evento catastrofico naturale oppure un attacco. Le compagnie resilienti predispongono di conseguenza piani e procedure per ridurre gli effetti dell'evento ed assicurare la continuità operativa, queste pratiche prendono il nome di «**business continuity plan**» e «**disaster recovery**».

Business continuity plan (BCP)
Il «business continuity plan», piano per la continuità del business, ha lo scopo principale di dettagliare le policy e le procedure per minimizzare gli impatti negativi sull'operatività di una compagnia a valle di un evento catastrofico / attacco, e ad assicurare la continuità delle operazioni svolte dalla compagnia anche in situazioni di emergenza.

Il business continuity plan (BCP) si compone di quattro step principali:
- Pianificazione e scopo
- **Business impact assessment (BIA)**, ovvero valutazione degli impatti sul business
- **Business planning**, ovvero piano di continuità operativa
- Approvazione ed implementazione

Business impact assessment (BIA)
È l'analisi degli impatti sul business. Il BIA ha lo scopo principale di identificare le risorse critiche di una compagnia e le potenziali minacce alle quali esse sono esposte. Inoltre, il BIA ha lo scopo di misurare la probabilità che tali minacce possano verificarsi e l'impatto che esse potrebbero avere sul business. Il BIA e conseguentemente la sua «misurazione» può seguire l'approccio qualitativo o quantitativo.
-**Identificazione delle priorità del business**: Da un punto di vista **qualitativo**, si potrebbero, di fatto, identificare le priorità in base alla loro criticità relativamente al business – dove agli asset a supporto del business viene assegnata una priorità superiore. Da un punto di vista **quantitativo**, si potrebbe invece creare una lista contenente tutti gli asset della compagnia ed assegnare ad ognuno di essi un valore monetario, chiamato «asset value» (AV) e successivamente assegnare una priorità in base al valore.

All'interno di questa fase si definiscono altri due valori quantitativi:
Maximum tolerable downtime (MTD): definito come il limite massimo di tempo durante il quale un business può non essere operativo senza causare danni irreparabili al business stesso.
Recovery time objective (RTO): definito come l'ammontare di tempo necessario a recuperare un sistema o una funzionalità di esso in caso di disastro.
Lo scopo del BCP è di assicurare che RTO <= MTD, ovvero che il tempo per recuperare un sistema o una funzionalità critica in caso di disastro sia minore del tempo limite «sopportabile» dal business, e superato il quale si avrebbero conseguenze permanenti sul business stesso.
-**Identificazione dei rischi:** Stimare il rischio che impatterebbe l'organizzazione in caso di disastro naturale o causato dall'uomo.
-**Valutazione della probabilità:** Una volta identificati i rischi che possono impattare sull'organizzazione, ad ognuno di essi si associa la probabilità che l'evento si verifichi. Se la probabilità è stimata in numero di volte che l'evento si è verificato nel corso di un anno, si parla di «annualized rate of occurrence» (ARO), ovvero tasso annuale di occorrenza.
I dati storici e le statistiche messe a disposizione degli enti pubblici possono sicuramente supportare la valutazione delle probabilità per quanto riguarda i disastri naturali.
-**Valutazione degli impatti:** Il risultato della fase è una misura qualitativa (basso, medio, alto) o quantitativa (e quindi espressa in forma monetaria) degli impatti sul business legati ad un determinato evento.
Da un punto di vista **quantitativo**: si assegna ad ogni asset quello che viene chiamato «exposure factor» (EF), misurato come la percentuale di asset che verrebbe impattato a seguito del verificarsi di un determinato evento, e si introduce il concetto di «single loss expectancy» (SLE), che ci dà una misura monetaria della perdita che si subirebbe al verificarsi dell'evento, calcolato come il prodotto tra il valore dell'asset (AV) e la percentuale impattata in caso di evento (EF): SLE = AV x EF
Se volessimo ora il valore della perdita subita in un arco temporale di un anno, chiamato ALE (annualized loss expectancy), dovremmo moltiplicare il valore del SLE per il numero di volte stimato dell'evento in un anno (ARO): ALE = SLE x ARO
Da un punto di vista **qualitativo**, invece, bisognerebbe considerare tutti gli impatti «non numerici» sul business come ad esempio: Pubblicità negativa (immaginate una banca che non riesce ad assicurare servizio agli intestatari dei conti corrente); Sfiducia dei clienti; Responsabilità etica e sociale dell'organizzazione. Non restituisce un numero in valuta, ma piuttosto una stima degli impatti sul business di un dato evento.

Business continuity planning
Ha lo scopo di sviluppare ed implementare una strategia per la riduzione dell'impatto dei rischi sugli asset protetti. Possiamo identificare le seguenti sottofasi:
Sviluppo della strategia: lo sviluppo della strategia è un'attività complementare all'identificazione delle priorità, discussa nella fase di BIA. Infatti, se nella BIA si identificano rischi ed asset prioritari, nella fase di sviluppo strategia si decidono i rischi che verranno gestiti all'interno del BCP. In questa fase il management deciderà quali rischi potrebbero essere accettabili, e quali invece no, quali rischi sono da evitare e quali invece inserire all'interno del BCP.

Stesura dei processi: all'interno di questa fase vengono dettagliati i processi e le procedure da seguire per la salvaguardia degli asset critici: personale, edifici ed infrastrutture. È bene ricordare che le persone sono sempre «l'asset» più significativo di una compagnia e pertanto devono essere dettagliati i processi per assicurare l'incolumità durante un'emergenza.

Abbiamo visto il BCP, che ha lo scopo di supportare le organizzazioni nella riduzione degli impatti sugli asset prioritari a valle di un evento critico (governance, pianificazione e gestione).

Disaster recovery planning (DRP)
Il **Disaster recovery planning (DRP)** può essere visto come il complemento tecnico al BCP che include i controlli tecnici da implementare per la riduzione del rischio e per il recupero dei servizi dopo un evento catastrofico.
Insieme, il BCP ed il DRP, servono da guida durante i momenti di crisi o emergenza per recuperare l'operatività del business quanto prima così da impattare gli utenti fruitori del servizio quanto più lievemente possibile.

Tecniche e dei controlli utilizzati in fase di disaster recovery
-**Resilienza dei sistemi**: i controlli tecnici che aumentano la resilienza di sistemi impattano positivamente sulla disponibilità di sistemi e servizi, uno dei principi cardine della triade CIA. Si definisce resilienza di un sistema la sua capacità di far fronte a determinati eventi critici. L'obiettivo primario dei controlli in esame è di eliminare i cosiddetti «single point of failure» (SPOF), intesi come quei componenti del sistema che possono causare anomalie o cessazione dell'intero sistema.
-Tolleranza agli errori: «fault tolerance» è la capacità di un sistema di continuare ad essere operativo nonostante un errore. Essa si può aumentare aggiungendo ad esempio componenti ridondanti all'interno dell'architettura, come ad esempio un disco in più per il salvataggio dei dati.
-**Protezione dei dischi**: la tolleranza agli errori e la resilienza di un sistema possono essere rinforzate come abbiamo visto aggiungendo ridondanza, per esempio eliminando SPOF causati da dischi rigidi unici, tramite l'inserimento di dischi aggiuntivi secondo la configurazione RAID. Un vettore RAID infatti, include 2 o più dischi per garantire continuità di servizio anche quando uno dei dischi non risulta più disponibile.
Il **concetto di ridondanza** può essere applicato a tutti gli asset critici, dove la ridondanza può dare un valore aggiunto al sistema. Quando parliamo di server, il concetto di ridondanza trova applicazione pratica nel «failover cluster», dove con cluster si intende un gruppo di computer che svolge generalmente lo stesso ruolo e che sono tra di loro sincronizzati, i singoli computer vengono chiamati anche nodi del cluster. Il «**failover cluster**» include due o più server e permette l'operatività dell'intero sistema anche a fronte di un errore su uno dei due server. Quando il server attivo smette di funzionare, l'altro nodo del cluster viene «promosso» a nodo attivo tramite un meccanismo automatico detto failover. Questo concetto può essere applicato a vari tipi di server ad esempio: web server che erogano servizi su internet, application server, database.
-Disponibilità elettrica: la tolleranza agli errori può essere applicata anche ai sistemi elettrici mediante l'utilizzo di generatori di corrente autonomi. Ad esempio se il data center che

ospita tutti i server della compagnia subisse una perdita di corrente elettrica potrebbe causare molti danni.
-**Backup**: un piano di disaster recovery deve assolutamente prevedere una strategia preventiva di backup. Ovvero una strategia di come copiare i dati, i sistemi e le configurazioni attualmente in produzione al fine di recuperare l'operatività a fronte di un disastro. Tra le strategie di backup troviamo: Full backup, Incremental backup, Differential backup.
-Migration to cloud: fenomeno tecnologico della migrazione dei server da on-premise (utilizzo di server fisici) al cloud. Ad oggi, ci sono molti cloud service provider (CSP) come Google, Amazon, Microsoft che mettono a disposizione servizi in Cloud per le compagnie. Di conseguenza la stesura di un piano di disaster recovery deve anche considerare l'approccio adottato. Una compagnia potrebbe avere una parte dell'infrastruttura nei propri datacenter e quindi gestirne la sicurezza e il piano di disastro ed una parte completamente demandata al cloud provider, che in tale caso sarebbe anche parte responsabile delle politiche di disaster recovery.

Threat Intelligence
La Threat Intelligence include le attività di raccolta di informazioni che provengono da fonti di diverso tipo in merito alle potenziali minacce che potrebbero impattare un sistema o una compagnia. I dati di potenziali nemici, le loro motivazioni, metodologie e strumenti a disposizione sono tutte informazioni fondamentali per capire da chi e come difendersi.

La classificazione delle minacce (threat classification) -> Uno dei modelli più utilizzati è il modello «**STRIDE**» di Microsoft per la **classificazione delle minacce**, dove ogni lettera rappresenta una categoria:
Spoofing of user identity, ovvero l'azione di impersonificare in maniera non autorizzata un utente valido di un sistema.
Tampering, ovvero l'azione non autorizzata di alterare un sistema causando danni ad esso o ad un suo componente.
Repudiation, che include tutte le minacce associate agli utenti che negano di eseguire un'azione senza che altre parti abbiano modo di provare il contrario, ad esempio, un utente esegue un'operazione illegale in un sistema che non ha la capacità di tracciare le operazioni vietate (tramite log per esempio).
Information disclosure, che si riferisce alla divulgazione di informazioni che implicano l'esposizione di dati e informazioni sensibili a persone che non dovrebbero avervi accesso, ad esempio la capacità degli utenti di leggere un file a cui non è stato concesso l'accesso.
Denial of Service, include tutte le minacce che volutamente causano indisponibilità di sistemi o servizi.
Elevation of privilege, che include tutte le minacce in cui un utente senza privilegi ottiene un accesso privilegiato ad un sistema così disponendo di privilegi sufficienti per distruggere o alterare/modificare l'intero sistema.

Le compagnie che vogliono capire a fondo la minaccia che potenzialmente potrebbero subire, possono inserire all'interno del loro piano annuale di sicurezza quello che viene

chiamato «**threat modeling**», dove vengono presi in esame diversi fattori al fine di capire i veri rischi per l'organizzazione.

Cosa succede se un attacco va a buon fine? Le compagnie generalmente rispondono con un piano che viene appunto chiamato «piano di risposta agli incidenti», o «**incident response plan**».

Gli indicatori di compromissione (IOC) sono utilizzati dai responsabili delle security operations e sono degli indicatori, ovvero dei segnali/delle evidenze degli attacchi per ricostruire uno storico e capire cosa è successo. Quindi comprendono lo studio di quei segnali che ci fanno capire che un evento potenzialmente dannoso si sta verificando o si è verificato su un sistema.
Vedremo i metodi utilizzati per identificare gli indicatori di compromissione che impattano:

- **Le reti** —> Analisi degli eventi Network
- **Gli end-point (e sistemi operativi)** —> Analisi degli eventi sugli host
- **Le applicazioni e i servizi** —> Analisi degli eventi applicativi o dei servizi

Analisi degli eventi Network:
La maggior parte degli incidenti di sicurezza vengono identificati grazie all'**analisi del traffico di rete** che mostra flussi inaspettati o comunque sospetti. I responsabili delle security operations devono essere abili a capire i segnali e ad analizzarli per far fronte all'incidente e ridurre gli impatti dove possibile.
Ci sono principalmente tre metodi piuttosto comuni per ottenere visibilità sulla rete e sul traffico che sono:

- Router-based monitoring
- Active monitoring
- Passive monitoring

Il monitoraggio attivo viene effettuato direttamente sul dispositivo, il monitoraggio passivo viene effettuato sul link.

Tra le tecniche di recupero flussi di rete ci sono infine i «**network monitoring tools**», ovvero i software utilizzati per lo sniffing delle comunicazioni su una rete come ad esempio **Wireshark.** Tra gli **indicatori di compromissione** che possono essere identificati con i tool appena visti al livello network troviamo:

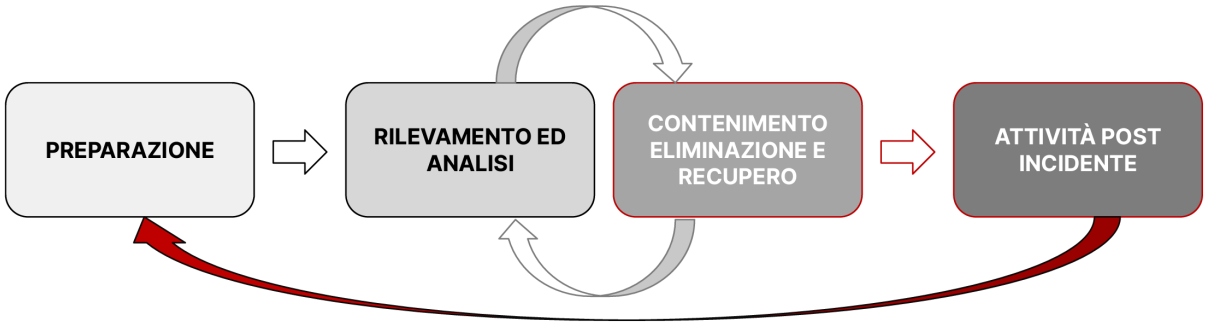
- **Consumo eccessivo della banda di rete** o delle schede di rete
- **Traffico in entrata da sorgenti piuttosto sospette** su porte critiche
- **Multiple richieste TCP su ampi intervalli di porte**, generalmente evidenza di una **scansione in corso**
- Numero molto elevato di **richieste TCP, UDP provenienti contemporaneamente da diversi indirizzi IP**, sintomo di un **Ddos in corso**

Analisi degli eventi sugli host:
Così come per le reti, anche per gli host possiamo identificare una serie di tool e tecniche note per supportare le analisi delle evidenze di attacchi in corso o già accaduti.
Tra le tecniche più comuni troviamo:

- Il monitoraggio continuo delle risorse di sistema: una tecnica molto basilare è il controllo delle risorse di un sistema per identificare eventuali attacchi esterni a fronte di un incremento ingiustificato dell'utilizzo computazionale.
- Monitoraggio dei processi: Alcuni attacchi avanzati riescono a «nascondersi» nel sistema operativo mostrandosi come dei processi leciti, il che rende praticamente impossibile la loro identificazione. Il monitoraggio dei processi ha il compito di monitorare il comportamento e le risorse utilizzate da ogni processo attivo al fine identificare eventuali anomalie.

Analisi degli eventi applicativi o dei servizi:
Un prerequisito per l'analisi degli eventi su applicazioni e servizi è conoscere esattamente il loro scopo, qual è il loro comportamento atteso e le risorse che servono per il loro funzionamento. Tra la **tecniche che permettono di identificare IOC** su applicazioni e servizi troviamo:
- **Log applicativi**: i log applicativi forniscono informazioni critiche su eventi che si verificano sull'applicativo, includendo informazioni di dettaglio sull'evento come data e ora in cui l'evento si è verificato, se è coinvolto un utente e così via.
- **L'analisi comportamentale**: identifica se un applicativo inizia a «funzionare» diversamente da quanto dovrebbe. Ad esempio, pensate ad un **attacco di tipo SQLi** dove un'applicazione inizia a restituire nome utente e password degli utenti.

Incident response



Il team responsabile di attuare il piano di risposta agli incidenti è il **CSIRTs, Computer Security Incident Response Teams**.

1. **Preparazione**

- Foundation: che include le attività relative alla preparazione delle policy e delle procedure di incident response
- Creazione del Team CSIRT: che include tutte le attività relative alla creazione del team di incident response, del training e degli aggiornamenti sulle nuove minacce.

Inoltre, nella fase di preparazione si definiscono anche i dispositivi ed i software necessari per eseguire le attività operative, come le workstation per la digital forensic, ovvero per

quelle attività mirate al recupero di informazioni dai sistemi operativi, dispositivi e memorie secondarie per il salvataggio di dati, stampanti e così via.
Una delle responsabilità maggiori che ha una compagnia durante la fase di preparazione di un piano di incident response è la **creazione di policy** e **procedure solide** per l'intero programma. Le policy forniscono una visione di alto livello sul processo di incident response, **le procedure** ne definiscono i **dettagli tecnici** utili al CSIRT durante la risposta ad un incidente di sicurezza.
Ogni qualvolta un incidente occorre, il CSIRT deve fornire una classificazione dell'incidente basata su diversi fattori come **tipo di incidente** e **criticità.**
I vettori di attacco per la classificazione degli incidenti:

- **External media**: si riferisce a tutti quegli attacchi che sono eseguiti da periferiche esterne, come una chiavetta USB ad esempio che inietta nel sistema codice malevolo.
- **Attrition**: include tutti quegli attacchi che utilizzano metodi di brute force per ottenere accessi non autenticati a sistemi ed applicazioni.
- **Web**: ricadono all'interno di questa categoria tutti gli attacchi eseguiti da un sito web o web-based, ad esempio un link malevolo in un URL.
- **Email**: include tutti quegli attacchi che si propagano per mezzo della posta elettronica ad esempio le campagne di phishing.
- **Impersonation**: include tutti quegli attacchi dove una risorsa, un'utenza o qualsiasi altro oggetto lecito viene sostituito o rimpiazzato con qualcosa di malevolo. Un esempio è il man-in the middle, MITM.

Il secondo fattore di categorizzazione degli incidenti è la **criticità**, ovvero l'impatto negativo sugli asset della compagnia sia in termini funzionali che in termini monetari.

2. Rilevamento ed analisi

La fase di rilevamento ed analisi è una delle più complicate da gestire come un processo automatizzato e continuativo di routine.
Tra gli **indicatori di attacchi in corso** troviamo:

- Gli **alert** che hanno origine da un sistema di prevenzione e rilevamento intrusioni (IPS/IDS) o da un SIEM o da un sistema antivirus. Gli alert automatici «scattano» quando un evento sospetto si manifesta.
- I **Log** generati da un sistema operativo, da un servizio o da un'applicazione, un dispositivo di rete e tutti i dispositivi hardware e software che sono in grado di produrre log.
- **Informazioni pubbliche** circa nuove vulnerabilità ed exploit appena scoperti (**0-day**), o scoperti in ambienti controllati.
- **Persone interne o esterne** alla compagnia che riportano **attività sospette** che potrebbero indicare un incidente di sicurezza in corso.

Quando una delle evidenze appena viste diventa concreta, il team CSIRT deve repentinamente iniziare la procedura di analisi e rilevamento per confermare che l'incidente è in corso.
L'**analisi** è un processo piuttosto complesso che può essere supportato da alcune azioni per migliorare l'efficacia:

- **Profilazione delle rete e dei sistemi**: quest'attività consente di migliorare l'abilità di un organizzazione di identificare attività sospette all'interno delle rete e dei sistemi.
- **Implementazione di tool UEBA**: i tool UEBA, «user and entity behavior analytics», sono software sviluppati per profilare il comportamento degli utenti al fine di identificare eventuali attività sospette.
- **Creazione di policy di logging efficaci**: i log devono contenere tutte le informazioni importanti, come il log-in log-out degli utenti e le modifiche amministrative.
- **Correlazione degli eventi**: la correlazione degli eventi da sorgenti multiple consente di tracciare tutti i passi di un eventuale attacco in corso, così identificando eventuali punti di accesso sulla rete o sui sistemi ed ogni modifica apportata. Generalmente la correlazione è a carico dei SIEM/SOAR.
- **Cattura del traffico**: se non è prevista dalla compagnia una cattura del traffico continuativa, una volta verificato un incidente di sicurezza il team CSIRT deve subito iniziare una cattura di tutto il traffico per successiva analisi.

3. Contenimento, eliminazione e recupero

Durante la fase di rilevamento ed analisi il team CSIRT mette in atto le prime attività per scoprire come è avvenuto l'incidente, quali sistemi ha impattato e quali potrebbero essere i prossimi sistemi a rischio. Una volta completate la valutazioni, il team deve trovare una soluzione per ridurre a stretto giro gli impatti dell'incidente.
Inizia la fase di contenimento, eliminazione e recupero che ha come scopo principale:

- La riduzione degli impatti causati dall'incidente (contenimento
- L'eliminazione dell'incidente dalla rete e dai sistemi
- Il recupero dei servizi e delle operatività standard

La riduzione degli impatti causati dall'incidente

Il primo step della terza fase di un piano di risposta agli incidenti è il contenimento del danno causato dall'incidente di sicurezza, che deve iniziare quanto prima possibile una volta terminata la fase di analisi. Le attività di contenimento hanno lo scopo primario di **isolare l'incidente** in modo tale che non possa creare ulteriori danni a reti/sistemi.
Ad esempio, se un computer su una rete è stato infettato con un malware, la prima attività per contenere gli impatti è isolare il sistema rispetto al resto della rete in modo tale che il malware non si riproduca su altri nodi.

Una delle tecniche preventive e strategiche per la gestione degli incidenti di sicurezza sulla rete è la «**segmentazione**», che risulta essere particolarmente utile anche nella fase di contenimento di un incidente in corso. La segmentazione include tutte quelle attività che permettono di **dividere una rete in diverse LAN o VLAN**. Ad esempio, supponiamo che il sistema C sia stato infettato da un malware. Allo stato attuale, se il malware fosse in grado di riprodursi potrebbe infettare anche A,B e D. La segmentazione permette invece di separare il sistema C dagli altri computer sulla rete, creando una rete ad hoc, che viene chiamata generalmente «**rete di quarantena**».
Con le dovute configurazioni a livello network, il malware risulterebbe così separato dal resto della rete ed incapace di riprodursi.

Sebbene la segmentazione riesca a limitare la riproduzione del malware e l'accesso al resto della rete da parte dell'attaccante, spesso non è sufficiente per chiudere la fase di contenimento. Quando è necessario un contenimento maggiore, si utilizza la tecnica dell'**isolamento.** L'isolamento consiste nella completa disconnessione del sistema infetto dalla rete, per restringere ancora maggiormente l'accesso alla rete interna da parte dell'attaccante. In questo scenario l'attaccante ha ancora accesso al sistema C tramite Internet. Ci sono casi in cui l'isolamento non è ancora abbastanza. In questi casi si procede con la tecnica di contenimento più stringente, ovvero la completa **rimozione del sistema dalla rete** sia Interna sia Internet. In quest'ultimo scenario l'attaccante non avrà né accesso alla rete interna né tantomeno alla macchina infettata.

Dopo le attività di contenimento, il tema CSIRT deve passare alla fase di **rimozione dell'incidente**. In questa fase lo scopo è eliminare tutte le attività, le componenti, i processi che restano dell'incidente all'interno della rete o sui sistemi.
Questa attività può includere ad esempio rimuovere eventuali backdoor installate da un malware, oppure ripulire dischi e chiavette usb compromesse.

Una volta completata la rimozione dell'incidente dalla rete e dai sistemi impattati, inizia la **fase di recupero**. La fase di recupero consiste nel ristabilire la normale operatività delle applicazioni e dei servizi. Include ad esempio il recupero dei dati e delle informazioni perse, l'applicazione delle patch dove disponibili per eventuali sistemi obsoleti, la revisione delle politiche dei firewall, IPS e IDS oppure l'aggiornamento delle firme degli antivirus. Infatti, lo scopo della fase di recupero è anche quello di evitare che lo stesso attacco possa capitare nuovamente in futuro.

Per quanto riguarda i sistemi, server e host, se sono stati compromessi da un attaccante durante un attacco dovrebbero essere considerati non più affidabili e dovrebbero essere di conseguenza ripuliti a fondo prima di essere utilizzati nuovamente.
A tale scopo, si utilizzano le tecniche di «reconstruction» o «rebuilding».
Reconstruction: include tutte quelle attività che mirano a recuperare quelle parti ancora affidabili di un sistema compromesso.
Rebuilding: include tutte quelle attività che mirano a ricostruire interamente un sistema impattato considerato non più affidabile.

Per quanto riguarda invece applicazioni, server e software, prima di procedere con la fase di recupero bisogna capire qual è stato il **punto di ingresso**, per capire dove sono presenti eventuali scoperture di sicurezza per implementare le patch ed evitare che lo stesso incidente possa capitare in futuro.
Il processo di analisi e patching dei sistemi di cui sopra, segue la priorità nella figura di seguito (1 = max priorità, 2, 3).

Durante la fase di recupero, ci si trova spesso a dover **gestire lo smaltimento o il riutilizzo di un disco o un sistema di storage di un sistema compromesso**. In questo caso bisogna accertarsi in prima istanza che le informazioni presenti sul disco/componente siano completamente inaccessibili prima di smaltire/utilizzare nuovamente il disco.

Generalmente, possiamo individuare tre **opzioni per la gestione dei media contenenti informazioni sensibili**:

- **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. Questo metodo è sicuramente il più efficace per rendere le informazioni inaccessibili ma è anche quello che comporta un effort in termini economici maggiore.

Questa è la differenza tra Purge e Destroy per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi.

4. Attività post-incidente

L'ultima fase di un piano di incident response è la fase post-incidente dove si fanno delle considerazioni su cosa poteva esser fatto meglio, cosa poteva esser fatto per evitare determinate situazioni. Quest'analisi post-incident viene detta «**lesson learnt**».

SQL Injection

Un SQL injection è una categoria di attacchi informatici in cui un attaccante inserisce o manipola comandi SQL in campi di input di un'applicazione web, al fine di compromettere la sicurezza del sistema e ottenere accesso non autorizzato ai dati nel server sottostante.
Il risultato di questi attacchi è, quindi, il controllo sui comandi SQL utilizzati da una applicazione web. Ci sono due tipi di SQL Injection:

- **SQL Injection:** è l'attacco che comporta l'inserimento di una query SQL (Structured Query Language) malevola, in campi di input di un'applicazione web, per valutare la presenza di una vulnerabilità. In caso di risposta affermativa, l'inserimento di query malevole consente di estrapolare i dati dal server sottostante, il quale produrrà immediatamente in output i dati richiesti.
- **SQL Injection Blind:** rappresenta una forma avanzata di SQL injection in cui l'applicazione web non fornisce direttamente i dati all'attaccante. In altre parole, l'applicazione web non restituisce subito le informazioni richieste dall'attaccante attraverso le query, complicando il processo di conferma della presenza di una vulnerabilità. In questa situazione, l'attaccante, non ricevendo feedback immediato sulla riuscita dell'injection, deve testare il comportamento del sistema inserendo varie query e valutando le risposte, senza una conferma diretta della presenza della vulnerabilità. Nonostante ciò, strutturando bene l'attacco, l'attaccante può ottenere non solo l'estrapolazione dei dati ma anche la possibilità di manipolazione (modifica) dei dati presenti sul server stesso.

XSS (Cross-Site-Scripting)

L'**attacco XSS (Cross-Site-Scripting)** è un tipo di attacco informatico che consiste nell'inserimento di script malevoli, sfruttando la vulnerabilità delle applicazioni web che si verifica quando queste consentono l'inserimento di input utenti non sicuri, senza prevederne la sanificazione.

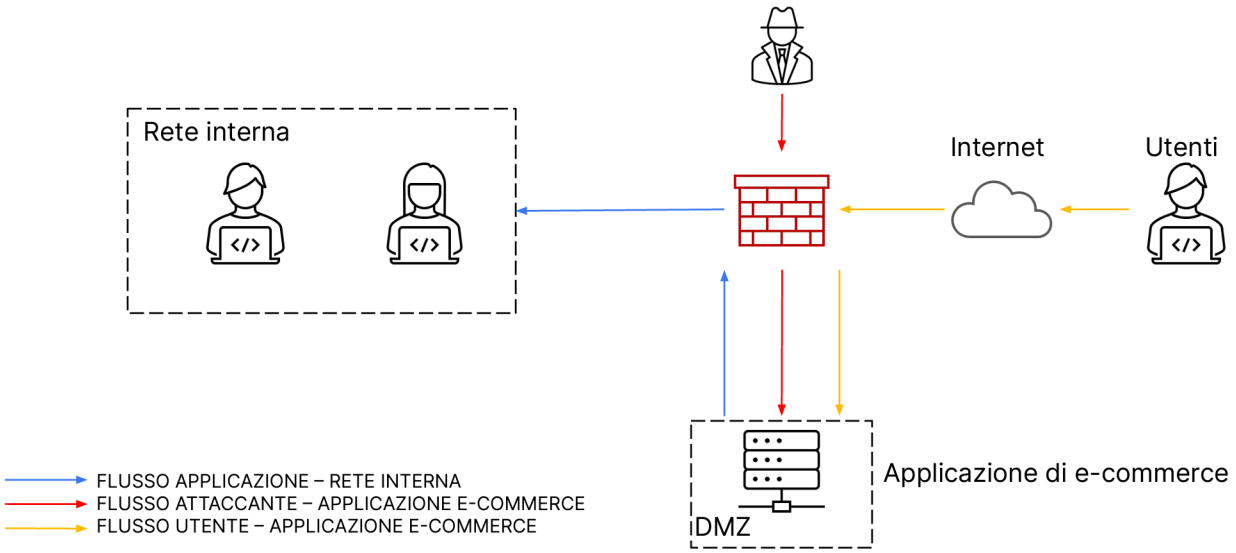
Due sono le tipologie più diffuse:

- **XSS Reflected:** In cui lo script dannoso viene immediatamente restituito sulla pagina web senza essere memorizzato sul server. Gli utenti vengono indotti a fare clic su un link contenente lo script, che viene, quindi, eseguito nel contesto del loro browser.
- **XSS Stored:** in cui gli script malevoli vengono immagazzinati sul server e restituiti in output ogni volta che un qualsiasi utente visiti una pagina specifica o acceda a un determinato elemento dell'applicazione. Nello specifico, l'applicazione web memorizza il codice malevolo all'interno del proprio server, diventando parte integrante della web app. Quando altri utenti accedono alle pagine web, il database restituisce in output il codice malevolo che viene eseguito dal browser degli utenti, dando inizio all'attacco. L'attacco XSS stored è molto pericoloso perché, a differenza di quello reflected, con un singolo attacco, si possono colpire diversi utenti di una data applicazione web e non è identificabili dai filtri dei web browser.

ESECUZIONE TASK

3. Azioni preventive

Analisi architettura della rete



Consideriamo che l'hacker è esterno e deve passare da Internet per entrare, superare il firewall e arrivare all'applicazione di e-commerce.

Nella rete troviamo:

Rete Interna:

- **Scopo:** La rete interna è la parte principale della rete aziendale, dove risiedono le risorse aziendali, i dati sensibili e le operazioni quotidiane.
- **Funzione:** La rete interna gestisce e protegge le risorse aziendali, tra cui server dei database, applicazioni aziendali, file con dati sensibili e dispositivi degli utenti. Qui si trovano anche server di autenticazione, server di file, stampanti e altri servizi utilizzati internamente.

DMZ (Demilitarized Zone):

- **Scopo:** La DMZ è una zona della rete aziendale separata da reti interne e reti esterne, progettata per ospitare servizi pubblici o esposti all'esterno, come server web, server di posta elettronica, server FTP, ecc.
- **Funzione:** La DMZ fornisce uno strato aggiuntivo di sicurezza separando i servizi pubblici dai server interni, riducendo il rischio di accessi non autorizzati alla rete interna. Gli accessi alla DMZ sono controllati attraverso regole di firewall per permettere solo il traffico necessario.

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.

Gli attacchi SQL Injection (SQLi) e Cross-Site Scripting (XSS) sono due tipi di attacchi informatici che sfruttano vulnerabilità nei siti web e nelle applicazioni web per ottenere accesso non autorizzato a dati sensibili, modificare il comportamento delle applicazioni o compromettere la sicurezza degli utenti.

SQL INJECTION

Questo tipo di attacco si verifica quando il database interpreta in modo errato gli input di testo e li riconosce come se fossero query interne. L'attaccante vuole recuperare o bypassare i sistemi di difesa del database. L'SQLi sfrutta la mancanza di sanitizzazione dei dati in input, consentendo l'inserimento di comandi dannosi.

XSS

Nell'attacco XSS, un attaccante inietta script malevoli nelle pagine web visualizzate da altri utenti. Questi script vengono eseguiti nel contesto del browser della vittima.

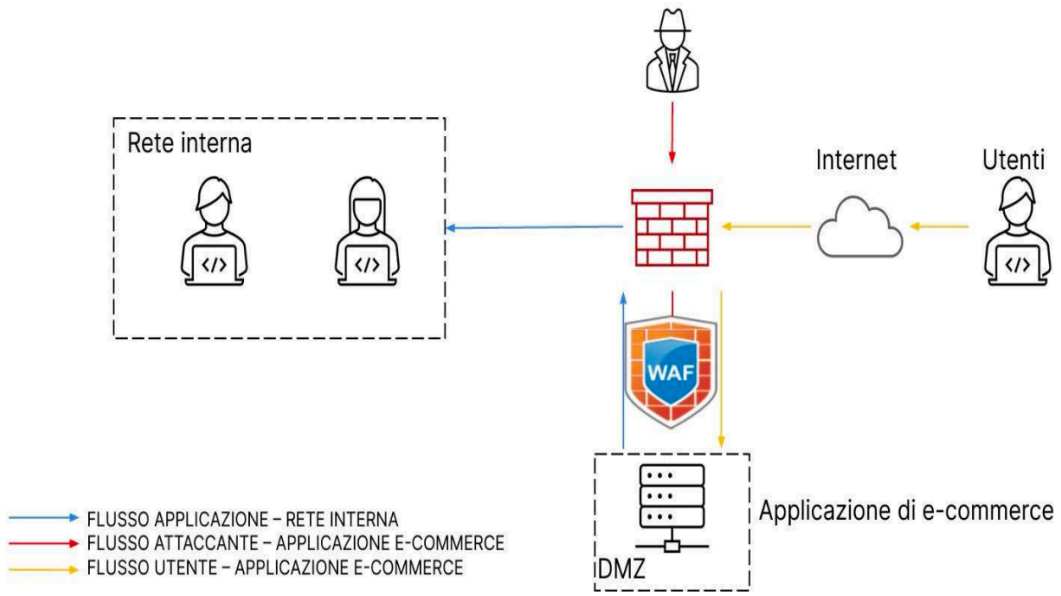
Implementazione delle azioni di prevenzione -> Modifico l'architettura di rete

Per difendere l'applicazione Web da attacchi di tipo XSS o SQLi da parte di un attaccante implemento un WAF (Web Application Firewall) che legge il contenuto di un pacchetto, lo confronta nel suo database e se è malevolo lo rigetta, in questo modo c'è una maggiore sicurezza per cercare di evitare eventuali attacchi provenienti dall'esterno.
Inoltre potrei potenziare le aree esterne al firewall (per esempio aggiungendo un IPS/IDS).

Il **Web Application Firewall (WAF)** è un tipo di firewall progettato per proteggere le applicazioni web da minacce, vulnerabilità e attacchi informatici. Si colloca tra la web application e il potenziale attaccante, analizzando e filtrando il traffico HTTP per prevenire violazioni della sicurezza e proteggere dati sensibili. Protegge applicazioni business-critical

e i server web da minacce come attacchi zero-day, attacchi DDoS (Distributed Denial-of-Service), SQL injection e XSS (Cross-Site Scripting).

Funzioni principali del Web Application Firewall (WAF): Filtraggio delle richieste e delle risposte in base a regole predefinite; Protezione contro attacchi comuni alle applicazioni web, come SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF); Validazione dei parametri delle richieste HTTP per garantire che siano conformi agli standard e previene l'inserimento di dati dannosi; Controllo degli accessi e autenticazione, limitando l'accesso solo a utenti autorizzati; Monitoraggio del traffico, identificando modelli di comportamento anomalo che potrebbero indicare attività sospette o tentativi di violazione; Logging e Reporting; Protezione della privacy; Aggiornamenti delle firme e delle regole; Integrazione con sistemi di sicurezza, collaborando con altri strumenti e sistemi di sicurezza per fornire una difesa più completa contro minacce e attacchi informatici.
Il Web Application Firewall è quindi un componente critico per garantire la sicurezza delle applicazioni web, proteggendo contro le minacce che possono sfruttare le vulnerabilità e compromettere l'integrità, la disponibilità e la riservatezza dei dati.
Inserisco il WAF subito dopo il firewall perimetrale:



Per garantire la protezione del web server che espone il servizio di e-commerce della compagnia ho aggiunto il WAF come in figura. Si deve, però, tenere presente che, per il corretto funzionamento del firewall, è necessario l'aggiornamento costante delle firme degli attacchi SQLi e XSS, che sono in costante evoluzione.

4. 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.

L'attacco di DDos è quell'attacco in cui il Denial of service viene effettuato simultaneamente da sorgenti multiple verso il target. Nello specifico, l'invio dell'ingente quantità di traffico di rete viene effettuato utilizzando una botnet. Quindi in un DDos la rete di dispositivi invia simultaneamente il traffico al server-target da diverse posizioni geografiche.
Il danno economico si calcola attraverso la seguente formula:
Danno Economico Totale= Tempo di Interruzione x Perdita Monetaria per Minuto

Facciamo il calcolo ->
Impatto sul business=1.500€ x 10 minuti =15.000€

Calcolare le perdite finanziarie, valutare l'impatto sulla reputazione del marchio e stimare i costi di mitigazione richiedono una comprensione approfondita dei processi di continuità operativa e di ripristino dai disastri.
Questo scenario sottolinea la necessità di strategie ben coordinate di Business Continuity e Disaster Recovery. In particolare, la strategia di ridondanza offerta dal Disaster Recovery Plan (DRP) emerge come una risorsa preziosa in queste situazioni.
Attraverso il DRP, che include la duplicazione e la distribuzione geografica delle risorse come i server, è possibile mantenere la continuità operativa durante un attacco DDoS.
Infatti, il concetto di ridondanza, applicata ad asset critici come i server, consiste nel prevedere un cluster di server, cioè un gruppo di server, spesso collocati in diverse aree geografiche, che hanno lo stesso ruolo e sono sincronizzati fra loro.
In questo modo, quando un server viene compromesso da un attacco di DDos, un altro prenderà il suo posto, garantendo la disponibilità del servizio e impedendo che si verifichi un impatto economico come quello calcolato nella presente esercitazione.

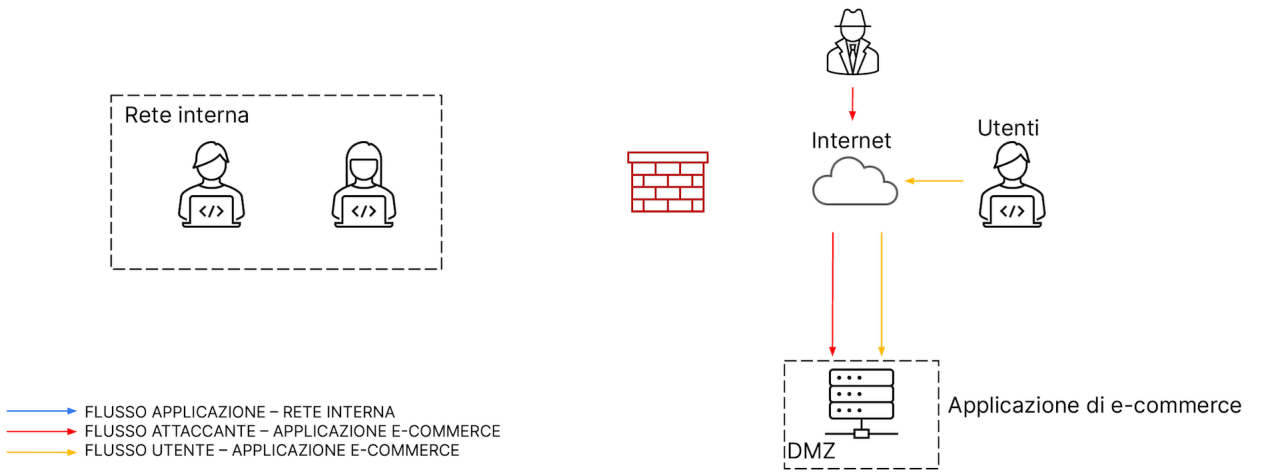
5. Response

L'**applicazione Web** viene infettata da un **malware**.
La **priorità** è che il malware non si propaghi sulla rete, mentre non siamo interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata.
Quindi vado a modificare l'architettura di rete:

La segmentazione riesce a limitare la riproduzione del malware e l'accesso al resto della rete da parte dell'attaccante, spesso però non è sufficiente per il contenimento. In questo caso è necessario un contenimento maggiore, utilizzo quindi la tecnica dell'**isolamento.**

L’isolamento consiste nella completa disconnessione del sistema infetto dalla rete, per restringere ancora maggiormente l’accesso alla rete interna da parte dell’attaccante.
L’Isolamento logico, invece, consiste nell’interrompere la comunicazione di rete tra il sistema compromesso e il resto della rete interna, modificando le configurazioni di rete o stabilendo policy, in firewall e altri dispositivi di rete, per impedire la connessione da e verso il sistema compromesso.

Per prevenire ulteriori danni causati dal malware e monitorare le azioni dell’attaccante, possiamo:
-SCOLLEGARE LA RETE INTERNA: tagliare le comunicazioni tra rete interna e server DMZ per prevenire il furto di dati e la propagazione del malware.
-MONITORAGGIO DELLE ATTIVITÀ: è necessario fare un monitoraggio costante per registrare i movimenti dell’attaccante sul server infetto, rilevare comportamenti sospetti o interessanti per l’analisi forense.



Non posizioniamo in rete di quarantena la Dmz perchè questo impedirebbe agli utenti di accedere. Notiamo che in questo scenario l’attaccante ha ancora accesso all’applicazione di e-commerce come richiesto.
Il motivo per cui non rimuoviamo l’accesso da parte dell’attaccante alla macchina infettata è perché economicamente all’azienda non converrebbe bloccare anche l’e-commerce.
Notiamo infatti che è permesso l’utilizzo dell’applicazione Web da parte degli utenti.