Report S9-L5

Analisi dei log: caso reale

Sommario

Traccia:

Con riferimento alla configurazione di rete fornita, 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.

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.

Abstract

Nel contesto di una settimana di studio focalizzata su aspetti chiave della sicurezza informatica nel contesto enterprise, la sicurezza delle applicazioni web emerge come un elemento cruciale. Durante questo periodo di formazione, sono stati approfonditi concetti fondamentali relativi a quattro pilastri strategici: le operazioni di sicurezza, la continuità operativa e il ripristino dai disastri, l'intelligence sulle minacce e la risposta agli incidenti.
Le tre esercitazioni in questione sono strettamente collegate a questi ambiti, ciascuna affrontando minacce specifiche e richiedendo l'implementazione di processi strategici.

Introduzione Teorica Generale

Sicurezza informatica "Enterprise"

È la disciplina dedicata alla protezione di sistemi informatici, reti, programmi e dati da minacce attacchi e accessi non autorizzati.

Scopo di questa "disciplina" è garantire la salvaguardia e protezione dei dati e, in particolare, la riservatezza, l'integrità e la disponibilità delle informazioni digitali.
Si tratta del trittico di principi fondamentali, definito CIA Principle, sulla base del quali viene valutato lo stato della sicurezza informatica.

CIA Principle

C = Confidentiality = riservatezza dei dati
Principio in base al quale l'accesso ai dati deve essere garantito solo agli utenti autorizzati.
La sicurezza informatica deve tutelare la riservatezza dei dati allo **scopo di prevenire o minimizzare gli accessi non autorizzati alle informazioni digitali**.
Le tecniche di tutela posso essere la cifratura e il controllo degli accessi.

I = Integrity = Integrità dei dati
È il secondo principio della CIA in base al quale le informazioni digitali devono mantenere l'accuratezza e completezza durante tutto il loro ciclo di vita.
La sicurezza informatica deve tutelare l'integrità dei dati allo **scopo di prevenire manipolazioni e modifiche non autorizzate dei dati**, in modo che in una comunicazione tra due parti, il dato ricevuto dal destinatario sia identico a quello inviato dal mittente.
Le tecniche di sicurezza sono: controlli di accesso o di autenticazione, verifica di hash e checksum.

A = Availability = Disponibilità dei dati
L'ultimo principio della Cia stabilisce che la disponibilità dei dati deve essere garantita in ogni momento, anche in caso di errore applicativo o crash dei sistemi, e per i soli utenti autorizzati ad accedere alle risorse.
La sicurezza informatica deve garantire che le risorse informatiche siano disponibili e accessibili, quando necessario, ai soli utenti autorizzati, allo **scopo di ridurre al minimo il rischio di interruzioni o attacchi che potrebbero renderle inaccessibili**.
Le tecniche di sicurezza sono: meccanismi anti Denial of service, back up, ridondanza infrastrutturale etc.

Per rischio o minaccia si intende la ***possibilità che un evento possa verificarsi***, causando danni totali o parziali a dati/informazioni/asset.

La gestione del rischio è di tre tipi:
1) Riduzione del rischio con le Security Remediation Actions (RA).
2) Accettazione del rischio.
3) Rimozione dell'asset (se non è critico) dall'infrastruttura aziendale.

SOC – Security Operations Center

È un sotto dipartimento all'interno del dipartimento di sicurezza informatica che si occupa delle operazioni di sicurezza, erogando, appunto, servizi per la protezione dei sistemi informatici, quali:

- **Servizi proattivi,** che includono tutte le attività che hanno lo scopo di rafforzare la sicurezza generale dell'infrastruttura aziendale**.**

- **Servizi di gestione della sicurezza informatica,** che includono le attività di gestione e manutenzione dell'infrastruttura IT delle compagnie.

- **Servizi di monitoraggio e risposta**, che includono le attività erogate al fine di monitorare in tempo reale tutte le componenti dell'infrastruttura IT.

Il monitoraggio ha lo scopo di individuare tempestivamente eventuali minacce informatiche.

L'attività di risposta agli incidenti di sicurezza in corso o verificatisi ha lo scopo di limitare i danni, cioè gli impatti negativi sul business della compagnia.

Per svolgere queste attività è necessario che, prima della verificazione dell'evento, si sia svolta la fase di **Threat Identification,** cioè di identificazione delle minacce alla sicurezza (security threats). Da notare, quindi, che si tratta di un processo che consente di identificare e analizzare il rischio che un evento dannoso possa verificarsi.
La fase di threat identification viene svolta usufruendo di un processo definito **Threat intelligence**.

Threat Intelligence (TI)

Definizione
Si tratta di un processo di ***raccolta, analisi e diffusione di informazioni sulle minacce informatiche per costruire una strategia di prevenzione o difesa da minacce che sia il più efficiente possibile.***
In sostanza, è un processo di identificazione e analisi delle cyberminacce.

Esistono tre categorie di Threat Intelligence:

- **Strategic intelligence**: che ha come obiettivo primario quello di fornire informazioni sulle minacce e sui potenziali attori delle minacce per fornire alle compagnie una vista complessiva su come e da chi difendersi.
- **Tactical intelligence**: che include dettagli tecnici e comportamentali da condividere con gli esperti di security per mettere in atto le azioni di risposta.
- **Operational intelligence**: che include, specificatamente, i dettagli per prevenire e rispondere alla singola minaccia, ma anche dettagli precisi sugli attori della minaccia, la sua provenienza ed i potenziali vettori d'attacco. Quindi, è un Intelligence orientato all'azione e che mira a supportare le attività operative in tempo reale.

La Threat intelligence supporta le Security operations fornendo, preventivamente, informazioni dettagliate sulle cyber minacce che potrebbero colpire un'organizzazione, al fine di migliorare le azioni di prevenzione degli attacchi informatici e delle successive risposte agli attacchi in corso.

Cenno a Business Continuity Plan (BCP)e Disaster Recovery Plan (DRP)

In tal senso, la TI è fondamentale per consentire di pianificare con anticipo i **Piani di Business Continuity e Disaster Recovery**, consentendo alle organizzazioni di comprendere meglio le minacce potenziali e di sviluppare strategie per garantire la continuità operativa in caso di eventi avversi.

Infatti, il **Business Continuity Plan (Piano di Continuità Operativa)** è un documento, redatto dalle organizzazioni, che definisce le procedure e le risorse necessarie per garantire la continuità delle operazioni aziendali in caso di eventi disruptivi (che causino interruzioni di operazioni e servizi). Include strategie per mitigare i rischi, gestire le emergenze e ripristinare le attività critiche affinché l'organizzazione possa continuare a funzionare in modo efficiente.

Il Disaster Recovery Plan (Piano di recupero) è, invece**,** complemento tecnico del Business Continuity Plan ed è focalizzato sul ripristino rapido e completo dei sistemi IT e delle infrastrutture tecnologiche, in seguito a un disastro o a un evento catastrofico.
Il DRP definisce le procedure, gli strumenti e le risorse necessarie per recuperare i dati e le operazioni IT, in modo che l'organizzazione possa riprendere le normali attività il più velocemente possibile dopo un'interruzione.

Azioni del SOC rispetto ad Incidenti di sicurezza e cenno alla correlazione con le esercitazioni del progetto

Si possono distinguere due tipologie di azioni adottabili dal SOC al verificarsi di incidenti di sicurezza, ovvero di eventi che impattino negativamente sulle organizzazioni come risultato dell'avverarsi di minacce avversarie, cioè di un attacco esterno o di un attacco interno volutamente dannoso (dipendente malevolo).
Si tratta di una distinzione basata sul posizionamento temporale rispetto agli incidenti di sicurezza e consiste in:

Azioni preventive: che sono le misure di sicurezza adottate per gestire e limitare le minacce di sicurezza, cioè il rischio che un evento dannoso si verifichi.

Di questa tipologia di azioni tratta il primo task affidato dalla traccia del progetto.

Azioni correttive e di risposta agli incidenti: che sono le azioni di rimedio per risolvere incidenti e ripristinare il corretto funzionamento dei sistemi informativi quanto prima.
Si tratta della cosiddetta fase di Incident Response.

Di questa tipologia di azioni trattano il secondo e terzo task affidato dalla traccia del progetto.

Incident Response Plan (IRP)

Nel caso in cui si verifichi un incidente di sicurezza, cioè la violazione ad un sistema informatico, come un attacco malware o un attacco di DDOS (anche se classificabile più come evento negativo disruptive), viene attivato il CISRT, il quale si occupa della risposta agli incidenti.

L’incident response indica la capacità operativa di identificazione, preparazione e risposta agli incidenti di sicurezza la quale viene concretizzata in un processo, eseguito sulla base del cd. “**Incident Respons Plan**”.
Il Piano di Risposta agli Incidenti, spesso redatto dal CSIRT, è un documento strategico e operativo che definisce le procedure e le azioni che un'organizzazione deve intraprendere in risposta a eventi di sicurezza informatica o a incidenti che potrebbero minacciare la sicurezza e la continuità operativa.

CSIRT e processo di Incident Response

Il **CSIRT** (Computer Security Incident Response Team) è un team, composto da impiegati, dirigenti e personale tecnico, responsabile di attuare il piano di risposta agli incidenti.

Il **processo di Incident Response** (di risposta agli incidenti) è ***finalizzato alla gestione della risposta agli incidenti di sicurezza dannosi*** in modo da limitare gli impatti negativi che questi generano, ripristinare rapidamente le operazioni e i servizi delle compagnie e apprendere dall’esperienza per evitare che gli stessi incidenti ricapitino in futuro.

Questo processo si compone di quattro fasi:

1) La **preparazione**, che include, a sua volta:
   - La fase (Foundation) in cui si stabiliscono le policy, cioè le linee guida generali e gli obiettivi da seguire durante le attività di risposta agli incidenti, e le procedure, che definiscono i dettagli tecnici utili al CSIRT durante le attività di risposta.
     Si delinea sostanzialmente il piano in Incident Response.
   - La fase di creazione del Team che include la creazione del team ,sempre che non ve ne sia già uno permanente, e le attività di training e aggiornamento sulle minacce informatiche.
   - Inoltre, si definiscono anche le risorse, dispositivi e software, che saranno necessari per svolgere le attività operative di recupero di informazioni dai sistemi operativi, dispositivi e così via.

2) **Rilevamento, Identificazione e Analisi**

   - **Il rilevamento** di attacchi in corso è il processo automatizzato e continuativo di identificazione della presenza di un attacco in corso.

   Viene effettuato utilizzando **indicatori di attacco** in corso quali:
   - alert da sistemi IDS/IPS, SIEM (log collector), e sistemi antivirus (come quando viene rilevato un attacco malware).
   - Log generati da OS, servizi, applicazioni, dispositivi di rete, hardware e software.
   - Informazioni su nuove vulnerabilità, scoperte a prescindere o grazie ad attacchi sconosciuti (0 day).
   - Suggerimenti di attività sospette provenienti da persone interne o esterne alla compagnia.

- Il CSIRT deve, poi, effettuare la classificazione delle minacce, usando, solitamente, due fattori di classificazione: il **tipo di incidente**, identificato tramite vettore di attacco, e la criticità.
  Per quanto attiene al 1° fattore, gli attacchi si dividono in:
  - **External media**: che si riferisce a tutti quegli attacchi che sono eseguiti da una periferica esterna, quale può essere una chiavetta USB, ad esempio, che inietta codice malevolo nel sistema.
  - **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 a mezzo 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).

  Per quanto riguarda il 2° fattore, il CSIRT deve categorizzare gli incidenti in base alla **criticità**, cioè all'impatto negativo sugli asset della compagnia sia in termini funzionali che in termini monetari.
  La criticità può essere:
  - **Inesistente**, se non si riscontrano interruzione sui servizi, che, essendo erogati a tutti gli utenti, non comportano perdite economiche
  - **Bassa**, se ci sono impatti ma i servizi critici della compagnia sono attivi e la perdita economica è limitata.
  - **Media**, se la compagnia non riesce ad erogare alcuni dei servizi critici o parte di essi ad un sottoinsieme limitato di utenti e questo comporta una perdita economica attesa non indifferente
  - **Alta,** la compagnia non riesce ad erogare servizi critici per nessuno degli utenti e la perdita economica attesa è molto pesante (superiore a 500.000€)

  Queste informazioni sono cruciali per adottare una risposta adeguata e definire le priorità nella gestione dell'incidente.

- L'**analisi** degli attacchi individuati e classificati è un processo piuttosto complesso che può essere implementato con azioni quali, a titolo esemplificativo, la profilazioni delle rete e dei sistemi, la profilazione dei comportamenti degli utenti (con tool UEBA) e la cattura continuativa del traffico di rete.

3) Contenimento, Rimozione e Ripristino

In questa fase il CSIRT deve trovare soluzioni per ridurre l'impatto degli incidenti, eliminare gli incidenti dalla rete e dai sistemi e recuperare i servizi, ripristinando l'operatività standard**.**

- Il 1° step, del **contenimento del danno**, comporta l'isolamento dell'incidente in modo tale che non possa creare ulteriori danni a reti/sistemi.

Le **tecniche** utilizzate sono la **segmentazione della rete, l'isolamento e la rimozione.**

- Successivamente, si procede all**'eliminazione di tutte le attività, le componenti e 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.
  La fase di rimozione dipende molto da che tipo di incidente di sicurezza è in corso.

- Una volta completata la rimozione dell'incidente dalla rete e dai sistemi impattati, inizia **la fase di recupero** che consiste nel **ristabilire la normale operatività** delle applicazioni e dei servizi, recuperando dati e informazioni perse, e nell'evitare che lo stesso attacco ricapiti in futuro, aggiornando, per esempio, le firme degli antivirus o revisionando la policy dei firewall.

  In questa fase, 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 o utilizzare nuovamente il disco.
  Per farlo ci sono tre diverse tecniche:

  - **Clear: in cui** il dispositivo viene completamente **ripulito** del 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, efficace ma anche più costoso ed aggressivo per lo smaltimento di dispositivi contenenti dati sensibili. In questo caso, infatti, oltre ai meccanismi logici e fisici appena visti, si utilizzano **anche tecniche di laboratorio** come *disintegrazione*, polverizzazione dei media ad alte temperature.

4) Analisi post-incidente

L'ultima fase dell'Incident response è quella nella quale si fanno **analisi post incidente**, cioè delle considerazioni su cosa poteva esser fatto meglio o cosa poteva esser fatto, più in generale, per rispondere e prevenire determinate situazioni.
Quest'analisi post-incident viene detta **«lesson learnt**», e ha lo scopo di imparare dagli errori o da eventuali mancanze per evitare che gli incidenti si ripropongano in futuro.

Infatti, le risultante di queste analisi serviranno da input per migliorare la fase di preparazione del **processo di incident response** che, quindi, **non è mai lineare** ma prevede dei cicli che permettono di tornare alle fasi precedenti, ove necessario.

Confronto tra Business Continuity Plan, Disaster Recovery Plan e Incident Response Plan.

A questo punto, ci si potrebbe chiedere allora se tutti e tre i piani, e relativi processi, debbano essere presenti nelle organizzazioni, visto che, in un'ottica generale, sembrano tutti e tre fare la stessa cosa: rilevare le minacce alla sicurezza, rilevare e identificare gli incidenti di sicurezza, determinare gli impatti negativi sul business (BCP e IRP) e rispondere agli attacchi, ripristinando l'operatività aziendale (BCP, IRP, DRP).

La risposta è positiva perché Business Continuity Plan, Disaster Recovery Plan e Incident Response Plan sono **processi che lavorano in sinergia, così come i team che ne sono responsabili, per garantire la sicurezza informatica a livello enterprise**.

Basti pensare al caso in cui sia in atto o sia concluso un processo di Incident Response.
A quel punto, a valle dell'evento critico, interverrà il processo e il piano di Disaster Recovery, che è specificamente designato per il ripristino di infrastrutture, applicazioni e servizi IT dopo un incidente o un episodio grave.
Un esempio di Disaster Recovery sono data center ridondanti distribuiti in più luoghi: se un data center viene distrutto, altri possono prendere il suo posto, assicurando la continuità di servizi e applicazioni.
Un altro esempio è il backup basato su cloud e un sistema di recovery che fa il backup automatico di tutti i dati e applicazioni essenziali su una macchina sicura offsite.

Si riporta una tabella in cui si può comprendere come sono attuati sinergicamente i tre piani durante un attacco informatico.

	Business Continuity	Disaster Recovery	Incident Response
Rilevamento	Mantenimento delle operazioni nonostante l'attacco.	Preparazione dei backup dei dati e dei sistemi critici.	Identificazione e risposta rapida alle intrusioni e alle anomalie.
Risposta	Monitoraggio costante per garantire la continuità operativa.	Verifica dell'integrità dei backup.	Isolamento delle risorse colpite per prevenire la diffusione dell'attacco.
Mitigazione e ripristino	Implementazione di misure correttive per garantire la sicurezza.	Convalida dell'ambiente ripristinato.	Monitoraggio e Implementazione di misure correttive permanenti.
Ripresa delle operazioni	Aggiornamento delle policy di sicurezza e delle procedure di business continuity.	Creazione di nuovi backup in base all'esperienza acquisita.	Restrizione dei privilegi di accesso.
Valutazione post-attacco	Analisi degli eventuali danni subiti e dei costi associati	Rapporti alle autorità competenti (se necessario) e comunicazione dell'avvenuto agli stakeholders	Analisi dettagliata e monitoraggio costante per prevenire ulteriori attacchi simili.

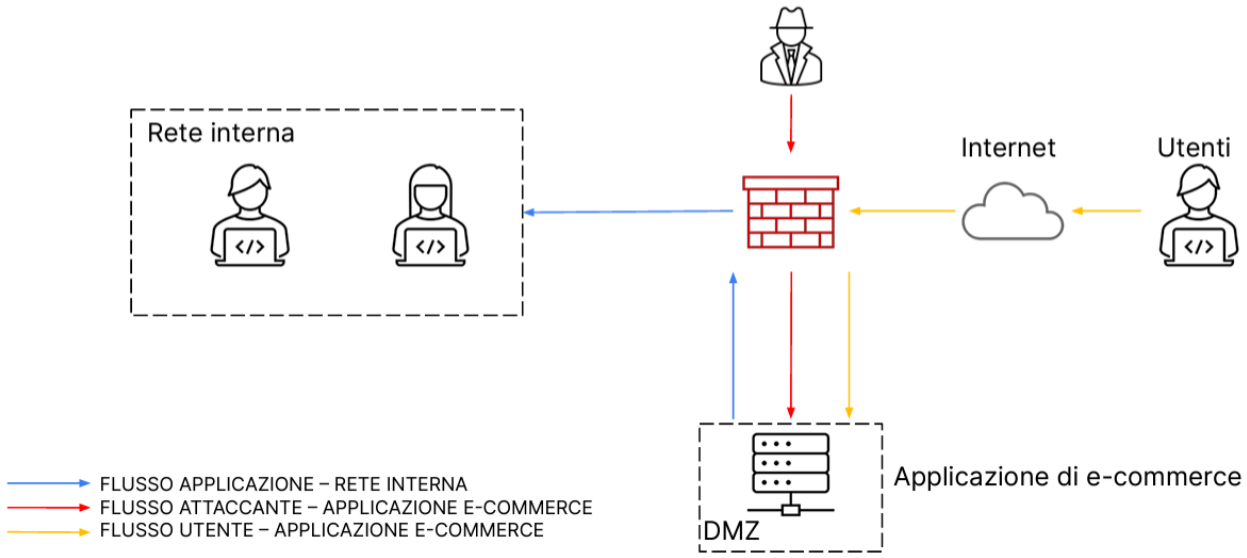
Svolgimento task del progetto

1° task – Azioni preventive

La traccia richiede, innanzitutto, con riferimento alla configurazione di rete fornita (**figura 1**), di rispondere al seguente quesito:

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.

Figura 1



Analisi architettura della rete aziendale

In questa configurazione di rete, si può notare che il malintenzionato, tramite internet, ha bypassato la sicurezza del **firewall perimetrale** a protezione della rete aziendale, per compromettere la sicurezza della DMZ (Demilitarized zone).

La **DMZ** è la zona di rete aziendale maggiormente esposta ad attacchi provenienti da internet, in quanto, ospitando il server su cui gira il servizio di e-commerce che la compagnia offre agli utenti, deve essere raggiungibile dall'esterno della rete e consentire la comunicazione in entrata e in uscita.

Nel caso riportato, il malintenzionato ha utilizzato un attacco SQLi o XSS, sfruttando l'assenza di adeguate azioni preventive che impediscano il verificarsi dell'incidente di sicurezza, cioè l'attacco, alla DMZ.
Si riporta, quindi, brevemente la descrizione delle due tipologie di attacchi per poi mostrare le soluzioni preventive al problema.

Attacchi SQLI e XSS

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**.

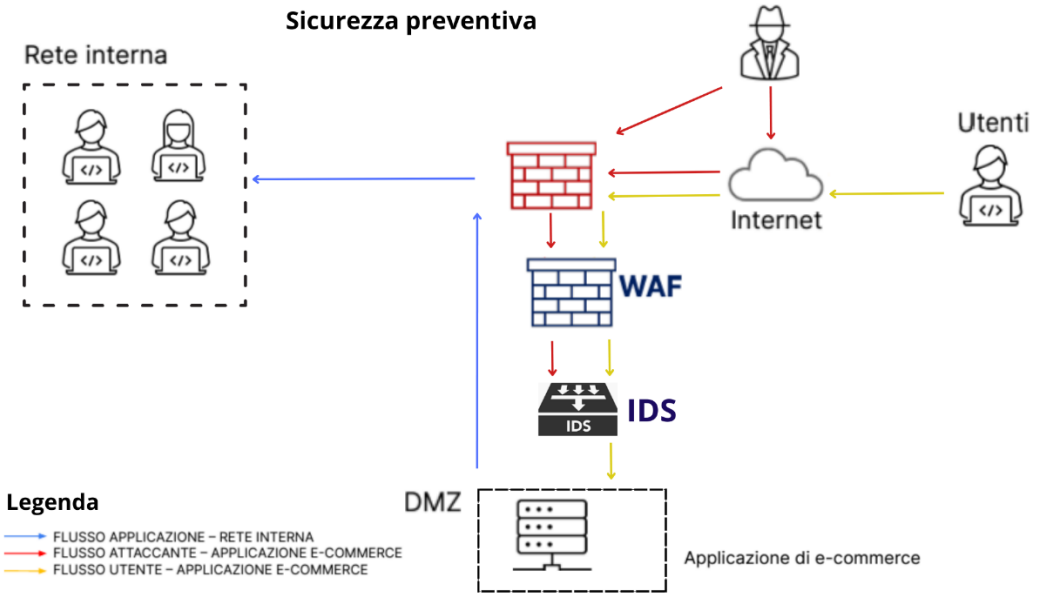
L'attacco XSS (Cross-Site-Scripting) è un tipo di attacco informatico che consiste nell'inserimento di script malevoli, sfruttando la vulnerabilità delle applicazioni web che si verifica quando queste consentono l'inserimento di input utenti non sicuri, senza prevederne la sanificazione.
Due sono le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

Implementazione delle Azioni di prevenzione

Figura 2



Il task affidato dalla traccia è strettamente collegato ad uno dei pilastri della sicurezza informatica, soprattutto di livello enterprise, ovvero l'implementazione di azioni preventive.

Le **azioni preventive** sono l'insieme dei controlli e misure di sicurezza adottate dalle compagnie per aumentare la protezione perimetrale ed interna dell'infrastruttura IT.
In particolare, tali azioni sono adottate prima del verificarsi di un incidente di sicurezza allo scopo di ridurre il rischio, la minaccia, la probabilità che gli attacchi informatici si verifichino.

Le azioni implementate nella **figura 2** sono un **WAF** (Web Application Firewall) **e un IDS (**Intrusion detection System**).**
Questi rientrano nei **controlli network,** deputati a **mitigare il rischio di attacchi alla rete aziendale,** che rappresenta il principale punto di accesso dei malintenzionati.

WAF: è il firewall progettato specificatamente per proteggere le app web ***filtrando, monitorando e bloccando in tempo reale qualsiasi traffico HTTP/HTTPS dannoso in entrata, impedendo, al contempo, l'uscita di dati non autorizzati dall'applicazione***.
Di conseguenza, i WAF proteggono le 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).
Questo Firewall utilizza policy di sicurezza preconfigurate ma offre anche la possibilità di personalizzarle per identificare e bloccare potenziali minacce.
In particolare, Il WAF è in grado di rilevare modelli di comportamento sospetti o attività maliziose, consentendo alle web application di resistere agli attacchi comuni.
Il WAF può essere implementato come software, appliance on-premise (come dispositivo fisico installato localmente presso l'organizzazione) o come servizio basato su cloud.

IDS: il sistema di rilevamento delle intrusioni è progettato per ***rilevare e segnalare eventi o attività anomale nelle reti e nei sistemi informatici.***
Funziona monitorando il traffico di rete, i log di sistema e altro, alla ricerca di firme e modelli noti di attacco informatico (quali per esempio XSS e SQLi), comportamenti anomali o violazioni delle policy di sicurezza preconfigurate nell'IDS stesso.
In caso di minaccia, non interviene direttamente bloccando l'attacco in corso ma invia segnalazione agli amministratori di sistema.

Conclusioni

Per garantire la protezione del web server che espone il servizio di e-commerce della compagnia sono state implementate due azioni preventive di controllo dell'accesso alla DMZ e alla web application.

Il WAF è posto subito dopo il firewall perimetrale perché è in grado di impedire gli SQL injection, cioè i tentativi di manipolazione dei comandi o delle query eseguite sul backend del server , e gli XSS, proteggendo gli utenti dalla manipolazione di script lato client e da richieste non autorizzate.

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.

Qualora un attaccante dovesse superare i controlli del WAF, si è previsto un sistema di rilevamento e segnalazioni delle intrusioni (IDS) in modo da consentire una più approfondita analisi dell'attacco da parte degli amministratori di sistema.
Anche in questo caso, è fondamentale la corretta configurazione del dispositivo per garantire l'aggiornamento rispetto ai nuovi attacchi.

2° task – Impatti sul business in caso di verificazione di un attacco informatico

La traccia, successivamente, riferisce che l'applicazione Web subisce un attacco di tipo DDos dall'esterno che rende l'applicazione non raggiungibile per 10 minuti, e di rispondere alla seguente richiesta:

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.

Attacco DDos

Nel caso riportato, l'applicazione Web ha subito l'interruzione del servizio di e-commerce, un asset fondamentale per il business della società, reso irraggiungibile a seguito di un attacco di DDos proveniente da internet.

Intanto, si ricorda che l'**attacco DDos** (Distributed Denial of service) è una **versione avanzata** degli attacchi **Dos** (Denial of service).

Un attacco di **Denial of service** si caratterizza per l'**invio di una ingente quantità di traffico di rete** al server target, sovraccaricandolo e impedendogli di gestire ulteriori richieste.

Lo **scopo** è di **determinare l'interruzione**, mettendolo fuori uso, **di un servizio in esecuzione** sul sistema e di impedirne l'accesso legittimo**, rendendolo indisponibile agli utenti autorizzati**.

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.

Una **botnet** è una rete di dispositivi (computer, server dispositivi IoT etc.), detti anche **bot o zombie**, "reclutati" tramite infezione da malware, che consente ad un entità centralizzata, il Control and Command Server (CC Server), di controllare i dispositivi, al fine di eseguire attacchi distribuiti, cioè multi sorgente, causando impatti negativi sulla disponibilità dei servizi.

È esattamente quello che accade in un DDos, dove la rete di dispositivi invia simultaneamente il traffico al server-target da diverse posizioni geografiche.

Calcolo dell'impatto sul business dovuto all'indisponibilità del servizio

Il calcolo dell'impatto sul business derivante dalla indisponibilità di un servizio non è altro che la **stima del danno economico subito durante la durata dell'interruzione del servizio**.

Il danno economico si calcola attraverso la seguente formula:
Danno Economico Totale= *Tempo di Interruzione* **x** *Perdita Monetaria per Minuto*

Dove:

- **Il Tempo di Interruzione** è la durata totale dell'interruzione del servizio in minuti.

- **La Perdita Monetaria per Minuto** rappresenta la perdita economica associato a ogni minuto di interruzione del servizio.

Il risultato di questa operazione fornisce una stima del danno economico totale subito dalla società a causa dell'interruzione del servizio, basato sulla perdita monetaria associata al tempo di inattività.

Nel contesto dell'attacco DDoS che rende l'applicazione non raggiungibile per 10 minuti e considerando che gli utenti spendono in media 1.500 € al minuto sulla piattaforma di e-commerce, si possono applicare questi valori nella formula:

Danno Economico Totale = 10 minuti × 1.500 €/*minuto*
Danno Economico Totale= 15.000 €

Quindi, il danno economico totale causato dall'interruzione del servizio per 10 minuti a causa dell'attacco DDos è di **15.000 €**.

Nell'ambito di una classificazione dell'attacco di DDos, effettuata nel Incident Response, la **criticità** che comporta, cioè l'impatto negativo economico che questo ha sul business della società, è

considerata **media** perché l'impatto economico non è indifferente e l'impatto in termini funzionali, visto il tempo ristretto di inattività, non è sufficiente per considerarla alta.

L'analisi degli impatti sul business derivanti da un attacco DDoS è collegata alla Business continuity e al Disaster Recovery.
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.
Quindi l'operazione di calcolo degli impatti rappresenta il punto in cui il BCP, il DRP e l'IRP convergono.

Conclusioni

In sintesi, l'attacco DDoS ha causato un'immediata e rilevante perdita economica di 15.000 € durante l'interruzione del servizio di e-commerce per 10 minuti.
La valutazione della criticità, parte integrante dell'Incident Response, ha categorizzato l'attacco come di entità media, principalmente a causa dell'impatto finanziario significativo.

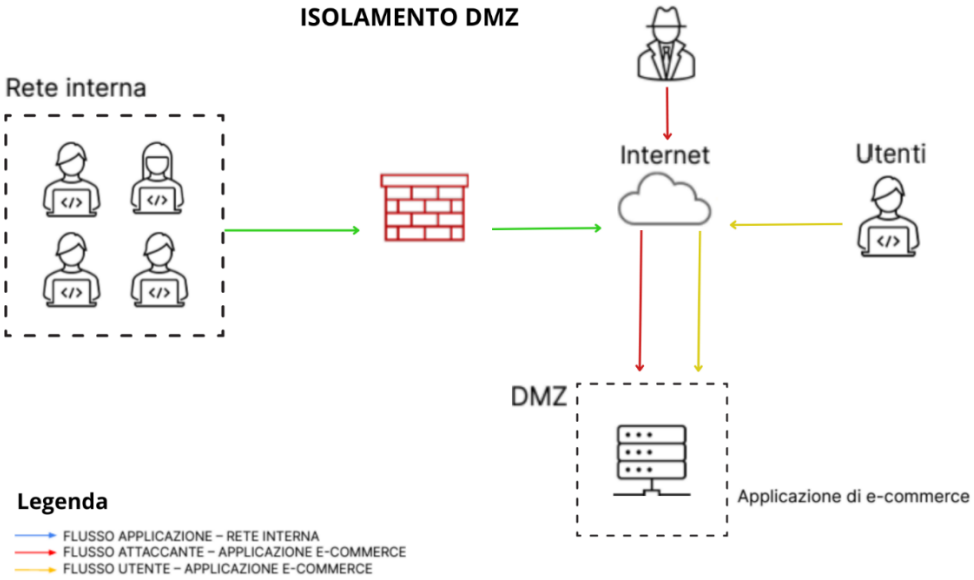
Questo scenario sottolinea la necessità di strategie ben coordinate di Business Continuity e Disaster Recovery.
In particolare, la **strategia di ridondanza** offerta dal **Disaster Recovery Plan** (DRP) emerge come una risorsa preziosa in queste situazioni.

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.

3°task – Response all'attacco malware

Infine, la traccia, tornando all'architettura di rete iniziale e senza considerare le soluzioni di sicurezza precedentemente implementate, riferisce che l'applicazione Web viene infettata da un malware.
Richiede, quindi, di effettuare delle modifiche in base al fatto che la priorità è che il malware non si propaghi sulla rete, senza rimuovere l'accesso da parte dell'attaccante al server infetto.



I malware, la categoria di attacco riportato in traccia**,** sono i **«**Malicious Software», ovvero **qualsiasi software** che viene **utilizzato con l'intento di procurare danno su un sistema operativo,** quali, fra i tanti**:**

- Causare «denial of service».
- Spiare l'attività degli utenti di un sistema.
- Ottenere controllo non autorizzato a dati e sistemi.

Per evitare la propagazione del malware, dal sistema operativo compromesso del server della DMZ alla rete interna, si è fatto riferimento al **processo di Incident response**, che è il processo di rilevamento, identificazione, e risposta agli incidenti di sicurezza**.**

Isolamento

Nell' architettura di rete modificata si è utilizzata la tecnica dell'isolamento, prevista come una delle possibili misure della fase di contenimento nell'ambito della risposta agli incidenti informatici. Questa fase è attivata dopo la rilevazione di un incidente di sicurezza e mira a contenere l'attacco malware, limitando i danni e prevenendo la sua diffusione.

L'isolamento consiste nella **completa disconnessione, logica e fisica, del sistema infetto dalla rete interna aziendale**, per impedire, rispetto alla semplice segmentazione di rete, **l'accesso alla rete interna da parte dell'attaccante**.

L’i**solamento fisico** implica il separare fisicamente il sistema compromesso dalla rete, scollegando i cavi di rete o interrompendo l'alimentazione elettrica.
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.

L'isolamento della DMZ, con il server del servizio e-commerce, se eseguito in modo tempestivo permette di **mitigare gli impatti dell'incidente**, **proteggendo,** al contempo, **la continuità operativa dell'organizzazione**.

È rilevante notare che, pur mantenendo l’attaccante accesso al server infettato da Internet, l'attacco non si diffonde alla rete interna, garantendo un livello di sicurezza e contenimento efficace.

Conclusioni

L'isolamento si configura come un'efficace strategia per prevenire la diffusione di malware, come evidenziato nel caso della DMZ, in quanto preserva l'integrità della rete interna, consentendo un contenimento efficace del malware.

Anche in questo caso, è necessario considerare l’integrazione di strategie di Disaster Recovery per garantire la continuità del business aziendale.

La ridondanza dei server, realizzata attraverso **cluster di server**, assicura la disponibilità continua del servizio critico di e-commerce, distribuendo il carico di lavoro in modo uniforme e garantendo una continuità operativa senza interruzioni prolungate. Infatti, nel caso della compromissione di un server, come quello attaccato dal malware, gli altri nodi del cluster subentrano automaticamente, assicurando la possibilità di continuare l’erogazione del servizio agli utenti.

Parallelamente, si deve implementare la pratica regolare di **backup**, che costituisce un pilastro essenziale della sicurezza informatica.
Il backup comporta la creazione di copie periodiche dei dati critici, memorizzandoli in posizioni sicure, in modo che, nel caso di attacco che comprometta l’integrità dei dati (come il malware), il ripristino da un backup recente consenta di recuperare rapidamente i dati, limitando i danni e garantendo una rapida ripresa delle operazioni.