

Analisi del Log: Real case

Indice:

1. Traccia;
2. Introduzione;
 - 2.1 Introduzione generica Security Operation;
 - 2.2 CIA;
 - 2.3 Cyber Minacce;
 - 2.4 Azioni Preventive;
3. Soc (Security operation center);
4. Siem e Soar;
5. Business continuity;
6. Disaster Recovery;
7. Le fasi dell'incident response;
 - 7.1 Preparazione;
 - 7.2 Rilevamento ed analisi;
 - 7.3 Contenimento, eliminazione e recupero;
 - 7.4 Post incident;
8. Task settimanali;
9. Conclusioni.



1. 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.
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.

2. Introduzione

Durante questa settimana ci siamo concentrati sugli aspetti cruciali della sicurezza informatica in contesti aziendali, la sicurezza delle applicazioni web si presenta come un elemento di vitale importanza. Nel corso di questa formazione, abbiamo esplorato concetti chiave relativi a quattro pilastri strategici:

1. La protezione informatica nell'ambiente aziendale;
2. La gestione della continuità operativa e del ripristino in caso di disastri;
3. L'analisi delle minacce e la pronta risposta agli incidenti.

Le tre sessioni pratiche sono strettamente connesse a questi ambiti, ognuna affrontando minacce specifiche e richiedendo l'attuazione di processi strategici.

Nel nostro caso specifico oggi andremo a testare i fondamentali dei concetti base della sicurezza informatica andando anche ad approfondire, oltre che le casistiche anche le figure fondamentali.

2.1 Security Operation

In sicurezza informatica, l'operazione di sicurezza (Security Operations) si riferisce all'insieme di attività e processi finalizzati a garantire la protezione, il monitoraggio e la risposta agli eventi di sicurezza all'interno di un ambiente informatico. Questa pratica è essenziale per identificare, gestire e mitigare le minacce alla sicurezza in tempo reale

L'operazione di sicurezza è fondamentale per mantenere un ambiente informatico sicuro e resiliente contro le minacce in continua evoluzione nel panorama della cybersecurity.

Questa pratica contribuisce a garantire che le organizzazioni siano pronte a fronteggiare e rispondere in modo efficace alle sfide della sicurezza informatica.

Le attività principali delle operazioni di sicurezza includono:

1. Monitoraggio: La costante supervisione di eventi di sicurezza attraverso l'utilizzo di strumenti e tecnologie che rilevano attività sospette o potenzialmente dannose.
2. Analisi degli incidenti: L'analisi dettagliata degli eventi rilevati al fine di determinare se costituiscano una minaccia effettiva e di comprendere la loro portata.
3. Risposta agli incidenti: L'attuazione di azioni correttive per mitigare gli effetti di un incidente di sicurezza, inclusa l'ispezione dell'origine dell'attacco e l'applicazione di contromisure.
4. Gestione delle vulnerabilità: Monitoraggio e risoluzione di vulnerabilità nel sistema per prevenire potenziali attacchi.
5. Gestione degli accessi: Controllo e monitoraggio degli accessi agli ambienti e ai dati sensibili, garantendo che solo le persone autorizzate possano accedervi.
6. Allerta tempestiva: Comunicazione immediata e adeguata alle parti interessate riguardo a eventi di sicurezza significativi o incidenti in corso.

2.2 CIA

In sicurezza informatica, CIA è un acronimo che rappresenta i tre principi fondamentali della sicurezza delle informazioni: **Confidentiality** (riservatezza), **Integrity** (integrità) e **Availability** (disponibilità). Questi principi costituiscono la base per la progettazione e l'implementazione di misure di sicurezza in un sistema o ambiente informatico.

L'obiettivo di implementare i principi CIA è quello di creare un ambiente informatico sicuro, equilibrando la protezione delle informazioni critiche con la necessità di renderle accessibili per scopi legittimi. Questi principi guidano la progettazione delle politiche di sicurezza, la selezione di controlli e tecnologie di sicurezza, nonché la gestione degli incidenti per preservare la sicurezza globale di un sistema o di un'organizzazione.

I principi fondamentali possono esser rappresentati come di seguito:

1. **Confidentiality** (Riservatezza): Si riferisce alla protezione delle informazioni da accessi non autorizzati. Garantire la riservatezza significa assicurarsi che solo le persone autorizzate abbiano accesso alle informazioni sensibili e che queste informazioni non siano divulgate a chi non ha il diritto di conoscerle.
2. **Integrity** (Integrità): Riguarda la protezione dell'accuratezza e dell'integrità delle informazioni. L'integrità assicura che i dati siano accurati, completi e non siano stati alterati in modo non autorizzato. Questo principio si concentra sulla prevenzione e rilevamento delle modifiche indesiderate ai dati.

3. **Availability** (Disponibilità): Indica che le informazioni e le risorse del sistema devono essere disponibili e accessibili quando necessario. La disponibilità si occupa di garantire che il sistema sia funzionante e accessibile agli utenti autorizzati, riducendo al minimo il rischio di interruzioni non pianificate.

2.3 Cyber Minacce

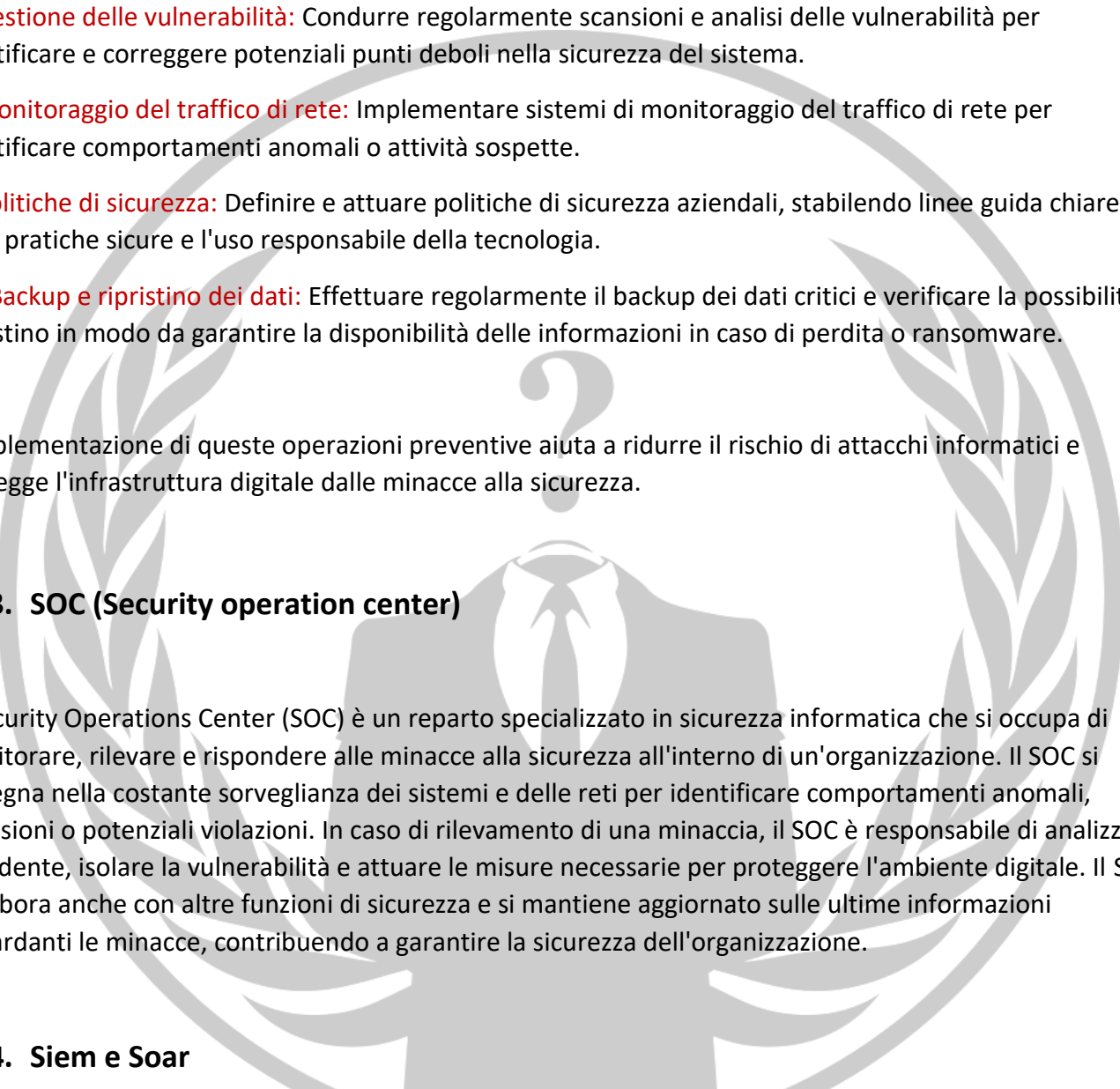
Nella cyber security i professionisti del settore devono essere a conoscenza dei maggiori vettori di attacco da parte dei malintenzionati affinché possano adottare le migliori contromisure per mitigare tali minacce. Tra i vettori di attacco più comuni possiamo trovare:

1. **Le botnets:** Una botnet è una rete di dispositivi informatici infettati da malware e controllati da un attaccante. Questi dispositivi, chiamati "bot," possono essere usati in modo coordinato per compiere attività dannose, come attacchi DDoS, diffusione di malware o furto di informazioni. Gli attaccanti gestiscono la botnet da remoto, utilizzandola per scopi criminali senza il consenso dei proprietari dei dispositivi infetti
2. **Denial of service:** Il Denial of Service (DoS) è un attacco informatico che mira a rendere inaccessibile un servizio o una risorsa online, sovraccaricandoli con un volume eccessivo di richieste, impedendo agli utenti legittimi di accedervi. L'obiettivo è negare il servizio a chi ne ha diritto, causando un'interruzione o un rallentamento delle operazioni.
3. **Zero day exploit:** Un "Zero-day exploit" è un attacco informatico che sfrutta una vulnerabilità di sicurezza sconosciuta, o zero-day, nel software. Questo significa che l'attacco avviene prima che gli sviluppatori abbiano avuto il tempo di creare una patch o un aggiornamento per correggere la falla, mettendo a rischio i sistemi non protetti.
4. **Man in the middle:** "Man-in-the-middle" è un attacco informatico in cui un terzo malintenzionato intercetta e manipola la comunicazione tra due parti senza che loro ne siano consapevoli. L'attaccante può leggere, alterare o iniettare dati nel flusso di comunicazione, compromettendo la sicurezza e la privacy delle informazioni scambiate.

2.4 Azioni Preventive

Le operazioni preventive in sicurezza informatica mirano a prevenire o mitigare potenziali minacce prima che possano causare danni. Alcune delle operazioni preventive comuni includono:

1. **Aggiornamenti e patch:** Mantenere tutti i software, sistemi operativi e applicazioni costantemente aggiornati con le ultime patch di sicurezza per correggere le vulnerabilità note.
2. **Firewall:** Configurare e utilizzare firewall per monitorare e controllare il traffico di rete, impedendo l'accesso non autorizzato o bloccando attività sospette.
3. **Antivirus e antimalware:** Installare e mantenere software antivirus e antimalware aggiornati per rilevare e rimuovere potenziali minacce da dispositivi e reti.

- 
4. **Controllo degli accessi:** Implementare politiche di controllo degli accessi per garantire che solo utenti autorizzati possano accedere a determinate risorse o dati sensibili.
 5. **Crittografia:** Utilizzare la crittografia per proteggere dati sensibili durante la trasmissione e nell'archiviazione, riducendo il rischio di accessi non autorizzati. Formazione degli utenti:
 6. **Fornire formazione** regolare agli utenti per aumentare la consapevolezza sulla sicurezza, insegnando loro a riconoscere e evitare minacce come phishing e social engineering.
 7. **Gestione delle vulnerabilità:** Condurre regolarmente scansioni e analisi delle vulnerabilità per identificare e correggere potenziali punti deboli nella sicurezza del sistema.
 8. **Monitoraggio del traffico di rete:** Implementare sistemi di monitoraggio del traffico di rete per identificare comportamenti anomali o attività sospette.
 9. **Politiche di sicurezza:** Definire e attuare politiche di sicurezza aziendali, stabilendo linee guida chiare sulle pratiche sicure e l'uso responsabile della tecnologia.
 10. **Backup e ripristino dei dati:** Effettuare regolarmente il backup dei dati critici e verificare la possibilità di ripristino in modo da garantire la disponibilità delle informazioni in caso di perdita o ransomware.

L'implementazione di queste operazioni preventive aiuta a ridurre il rischio di attacchi informatici e protegge l'infrastruttura digitale dalle minacce alla sicurezza.

3. SOC (Security operation center)

Il Security Operations Center (SOC) è un reparto specializzato in sicurezza informatica che si occupa di monitorare, rilevare e rispondere alle minacce alla sicurezza all'interno di un'organizzazione. Il SOC si impegna nella costante sorveglianza dei sistemi e delle reti per identificare comportamenti anomali, intrusioni o potenziali violazioni. In caso di rilevamento di una minaccia, il SOC è responsabile di analizzare l'incidente, isolare la vulnerabilità e attuare le misure necessarie per proteggere l'ambiente digitale. Il SOC collabora anche con altre funzioni di sicurezza e si mantiene aggiornato sulle ultime informazioni riguardanti le minacce, contribuendo a garantire la sicurezza dell'organizzazione.

4. Siem e Soar

SIEM (Security Information and Event Management) e SOAR (Security Orchestration, Automation, and Response) sono entrambe tecnologie utilizzate nel contesto della sicurezza informatica, ma hanno scopi e funzioni leggermente diversi.

SIEM (Security Information and Event Management):

Monitoraggio e Rilevamento: Raccoglie e analizza i dati provenienti da diverse fonti, come log di sistemi, dispositivi di rete e applicazioni, per identificare eventi di sicurezza e attività anomale.

Correlazione degli Eventi: Correla e analizza in tempo reale i dati per individuare pattern o comportamenti sospetti che potrebbero indicare una minaccia.

Generazione di Allarmi: Genera allarmi e avvisi in caso di attività considerate potenzialmente dannose o violazioni della sicurezza.

Archiviazione e Reportistica: Conserva i dati di sicurezza per fini di archiviazione a lungo termine e produce report per l'analisi delle tendenze e la conformità normativa.

SOAR (Security Orchestration, Automation, and Response):

Automazione delle Operazioni di Sicurezza: Automatizza le attività ripetitive e manuali svolte dai team di sicurezza, consentendo una risposta più rapida agli incidenti.

Orchestrazione dei Processi: Coordinazione di attività e flussi di lavoro tra diversi strumenti e sistemi per ottimizzare la gestione degli incidenti.

Risposta Guidata: Fornisce indicazioni e procedure guidate per aiutare gli analisti di sicurezza nelle decisioni e nelle azioni da intraprendere durante un incidente.

Integrazione dei Sistemi di Sicurezza: Si integra con altri strumenti di sicurezza e soluzioni per garantire una risposta coordinata e sinergica agli eventi.

In sintesi, mentre SIEM si concentra sulla raccolta, l'analisi e la segnalazione di eventi di sicurezza, SOAR va oltre, aggiungendo un livello di automazione e orchestrazione per migliorare l'efficienza nella gestione degli incidenti di sicurezza. L'integrazione di entrambe le tecnologie può fornire un approccio completo e avanzato alla sicurezza informatica, migliorando la capacità di rilevare, rispondere e mitigare le minacce in modo tempestivo ed efficiente.

5. Business continuity

La business continuity o "BC" nel contesto aziendale, è una disciplina che si occupa di garantire la disponibilità e la continuità delle operazioni di un'organizzazione in caso di eventi o incidenti che potrebbero minacciarle. L'obiettivo è ridurre al minimo l'impatto negativo su persone, processi, tecnologie e informazioni critiche per il business.

In termini di sicurezza informatica, la business continuity include le seguenti componenti:

Pianificazione e Preparazione: Definizione di procedure e piani per affrontare scenari di emergenza o interruzioni delle operazioni. Questo può includere piani di risposta agli incidenti, piani di recupero di emergenza e procedure di evacuazione.

Backup e Ripristino: Implementazione di strategie di backup regolari per garantire la disponibilità dei dati critici. In caso di perdita di dati o danni, i piani di ripristino vengono attivati per recuperare rapidamente le informazioni.

Ridondanza e Resilienza: Adozione di approcci che garantiscono la ridondanza delle risorse critiche. Questo può includere la distribuzione di sistemi su più siti geografici o l'utilizzo di infrastrutture ridondanti per garantire la continuità delle operazioni.

Test e Esercitazioni: Regolari test e simulazioni per garantire l'efficacia dei piani di business continuity. Queste attività consentono all'organizzazione di identificare e risolvere potenziali problemi prima che si verifichino situazioni di emergenza reali.

Gestione delle Crisi: Designazione di un team di gestione delle crisi responsabile di prendere decisioni rapide e coordinate durante eventi critici. Questo team supervisiona l'attuazione dei piani di business continuity.

L'integrazione di queste pratiche nella strategia di sicurezza informatica aiuta a proteggere le organizzazioni da interruzioni, perdite di dati e altri impatti negativi, garantendo al contempo la continuità delle attività anche in situazioni di emergenza.

6. Disaster Recovery

Per disaster recovery si intende il processo di pianificazione ed implementazione di misure per ripristinare le operazioni informatiche normali dopo un grave evento o un disastro che potrebbe causare interruzioni. L'obiettivo è minimizzare il tempo di inattività, recuperare i dati critici e assicurare che l'organizzazione possa tornare alle normali attività il più rapidamente possibile dopo un incidente, come ad esempio un attacco informatico, un guasto hardware o un disastro naturale.

7. Le fasi dell'incident response

Per quanto una azienda possa impegnarsi nel prevenire e preparare delle misure di sicurezza perimetrali la probabilità che un incidente si verifichi non è uguale a zero di conseguenza le aziende devono prendere in considerazione che un incidente prima o poi nel tempo capiterà e preparare di conseguenza quello che comunemente viene definito "incident response plan", ovvero il piano di risposta agli incidenti.

Le fasi più importanti di un incident response plan sono:

1. Preparazione;
2. Rilevamento ed analisi;

- 3. Contenimento, eliminazione e recupero;
- 4. Post incident;

7.1 Preparazione

Definizione dei Ruoli e delle Responsabilità: Identificazione dei membri del team di risposta agli incidenti e definizione dei loro ruoli e responsabilità.

Sviluppo dei Piani di Risposta: Creazione di procedure dettagliate per gestire specifici tipi di incidenti, con piani di risposta ben definiti.

7.2 Rilevamento ed analisi

Monitoraggio: Costante sorveglianza dei sistemi e delle reti per identificare comportamenti anomali o segni di possibili violazioni.

Analisi degli Indicatori di Compromissione (IoC): Esame degli IoC per determinare se c'è stata una violazione e per comprendere la portata dell'incidente.

7.3 Contenimento, eliminazione e recupero

Isolamento: Separazione delle parti compromesse o degli asset interessati per impedire la diffusione dell'incidente.

Riduzione del Danno: Attuazione di misure per minimizzare l'impatto dell'incidente e prevenire ulteriori danni.

Identificazione della Causa Radice: Individuazione della causa principale dell'incidente e attuazione di azioni correttive per rimuoverla definitivamente.

Ripristino dei Sistemi: Recupero dei sistemi interessati all'incidente per ripristinare la normale operatività.

7.4 Post incident

Analisi Post-incidente: Revisione dell'incidente per trarre insegnamenti e apportare miglioramenti ai processi di sicurezza.

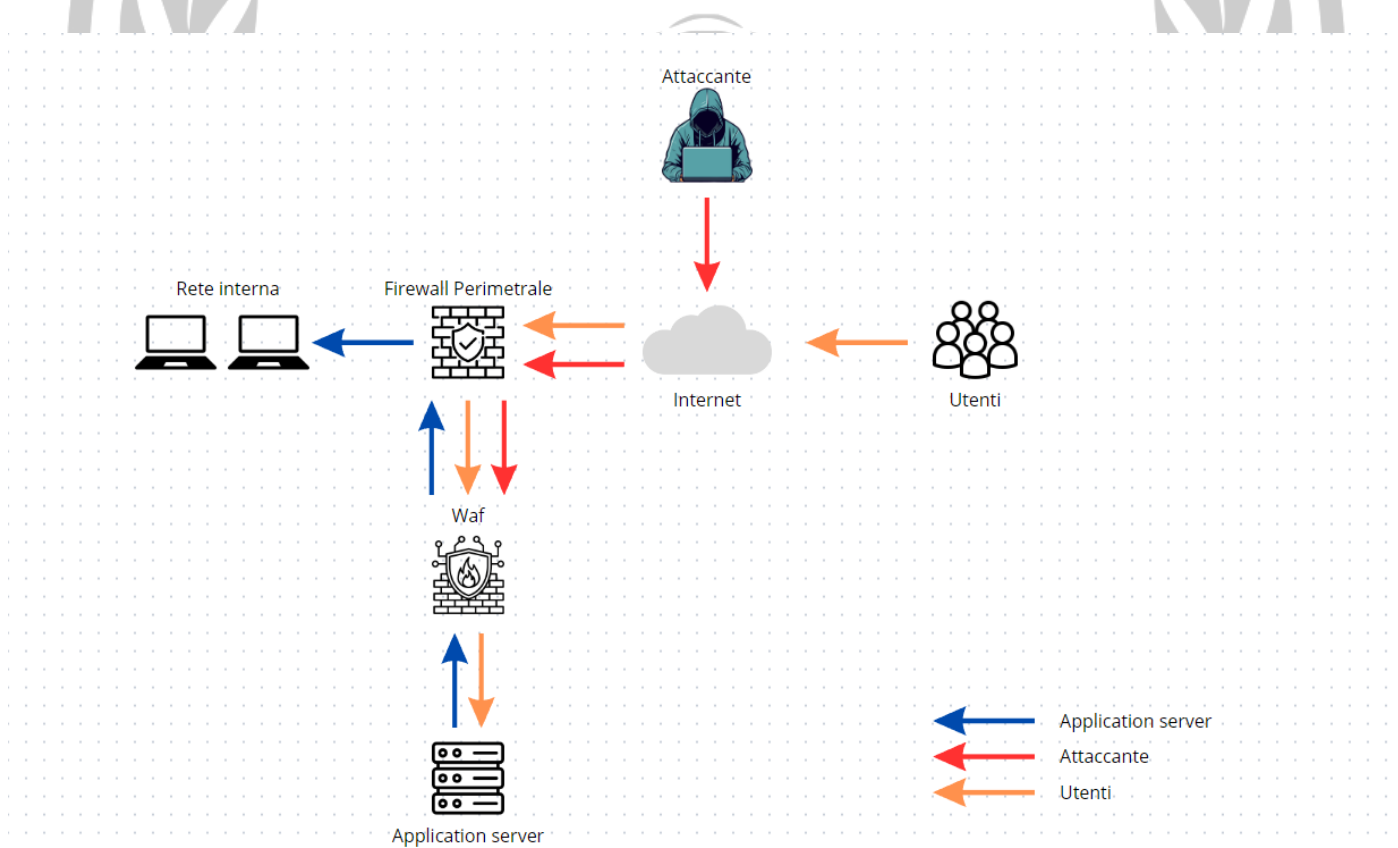
Documentazione dell'Incidente: Registrazione dettagliata di tutte le azioni intraprese durante la gestione dell'incidente.

Report post-incidente: Creazione di report dettagliati per comprendere le cause dell'incidente e per raccomandare azioni preventive future.

8. Task settimanali

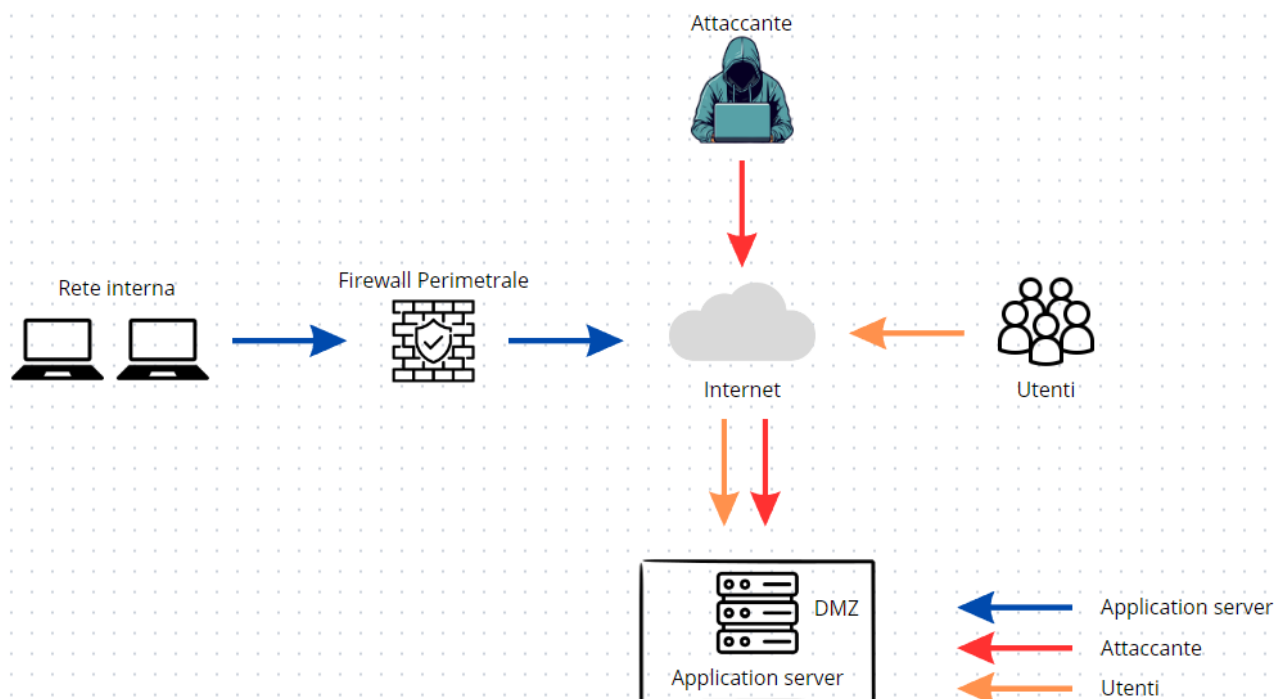
Dato lo scenario dell'esercizio fornito, ci concentriamo sull'attuazione di misure preventive per mitigare gli attacchi di tipo SQLi e XSS. Inoltre, intendiamo integrare un Web Application Firewall (WAF) per rafforzare la sicurezza. Il nostro obiettivo è prevenire futuri attacchi e limitare le perdite dovute al DDoS subito, affrontando in modo proattivo i rischi per la sicurezza informatica.

Di seguito la rappresentazione grafica della nostra casistica.

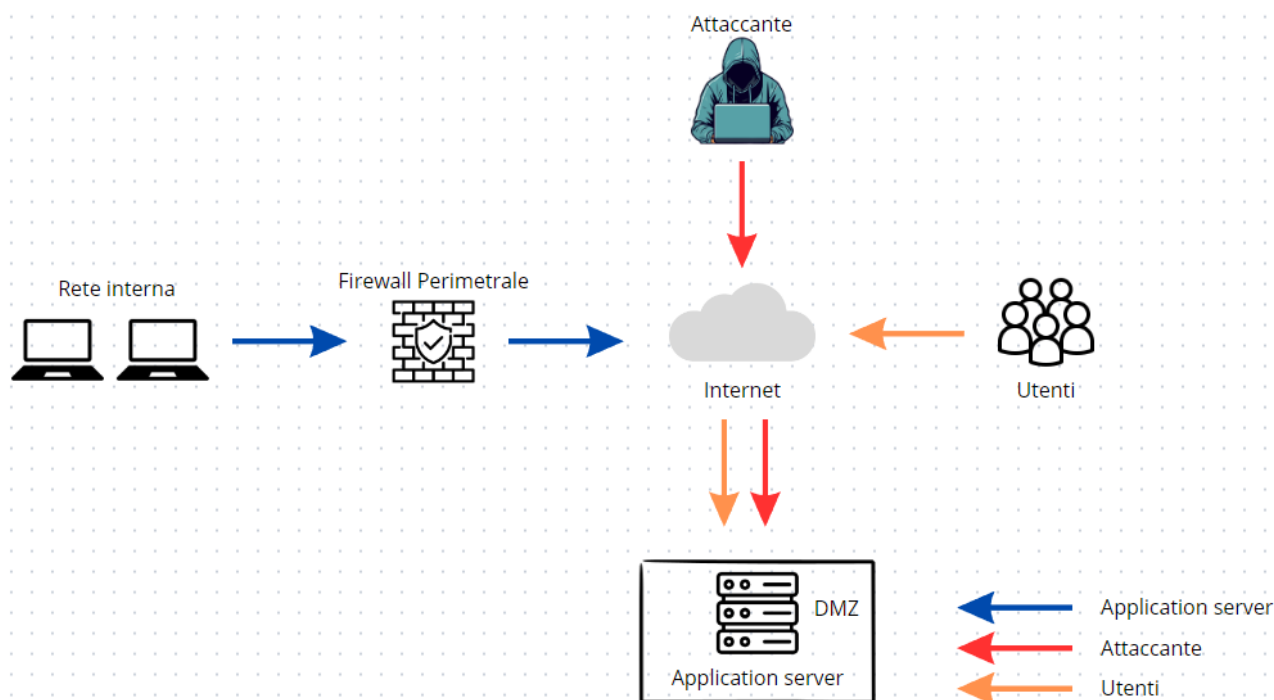


Successivamente, ci è richiesto di quantificare la perdita economica causata da un periodo di inattività di 10 minuti, considerando un guadagno medio di €1500,00. Il calcolo da eseguire consiste nell'applicare un moltiplicatore di tempo, ottenendo una perdita di €15.000,00 a causa dell'attacco DDoS.

Ora esaminiamo la situazione in cui il server è compromesso da un malware. Abbiamo scelto di adottare una strategia di isolamento del server e di implementare una politica firewall che impedisce al server di comunicare con la rete interna. Al contempo, consentiamo la connessione del server a Internet.



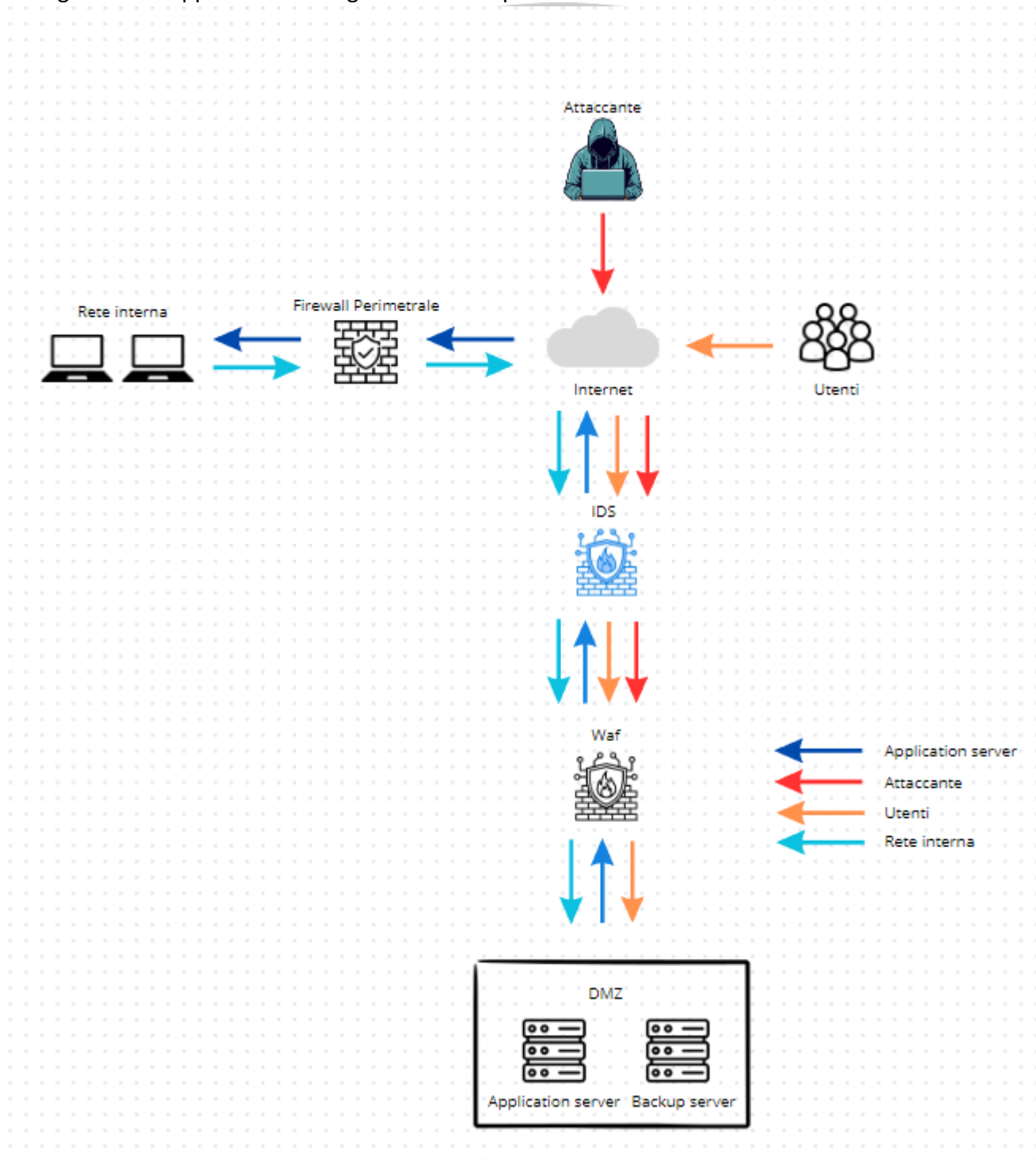
Ora ritornando alla prima casistica, andiamo ad effettuare una remediation per essa, andando ad alzare una policy al Firewall in modo tale che il Server Infetto non comunichi con la Rete Interna, andando anche ad implementare un WAF:



Infine, qualora fosse disponibile il budget necessario, ci proponiamo di apportare modifiche sostanziali alla struttura di rete. Questo coinvolgerà l'implementazione di un sistema di rilevamento delle intrusioni (IDS) per il controllo del traffico, l'uso di un Web Application Firewall (WAF) e l'introduzione di un Server di Backup.

Il Server di Backup sarà configurato per eseguire un backup completo del Server Principale ogni lunedì, mentre nel corso della settimana verranno effettuati backup differenziali. Questo server di backup fungerà da sostituto del Server Principale nel caso in cui quest'ultimo non sia in grado di erogare servizi.

Di seguito una rappresentazione grafica di esempio.



9. Conclusioni

In conclusione le azioni preventive dovrebbero concentrarsi sulla sicurezza dell'applicazione web attraverso controlli di input e l'uso di strumenti come WAF. La gestione di un attacco DDoS richiede la valutazione dell'impatto finanziario e la preparazione di strategie di risposta. Per quanto riguarda l'infezione da malware, isolare il server infetto e implementare un sistema di backup efficace sono fondamentali per mantenere l'integrità dei dati e la continuità delle operazioni. La sicurezza informatica richiede un approccio olistico, integrando azioni preventive, risposta agli incidenti e strategie di business continuity.

