1. Introduzione alla sicurezza web: SQLi e XSS

- ***Prevenzione contro SQL Injection (SQLi):***
- ***Query parametrizzate (Prepared Statements):*** Questa tecnica permette di separare l'input dell'utente dai comandi SQL, rendendo impossibile per un attaccante inserire codice SQL malevolo direttamente nel database. Utilizzare query parametrizzate è considerata una delle pratiche più sicure per prevenire SQLi.
- ***Validazione degli input:*** Implementare un sistema di validazione robusto per assicurarsi che gli input provenienti dall'utente non contengano sintassi pericolose o malevole. La validazione aiuta a bloccare immediatamente dati sospetti, riducendo i rischi di manipolazione del database.
- ***ORM (Object-Relational Mapping):*** Utilizzare strumenti di ORM non solo facilita l'interazione con il database, ma riduce la necessità di scrivere SQL grezzo, che può essere vulnerabile se non gestito correttamente. L'ORM crea un livello di astrazione tra l'applicazione e il database, rendendo le operazioni più sicure.
- ***Prevenzione contro Cross-Site Scripting (XSS):***
- ***Sanitizzazione degli input***: Rimuovere o codificare i caratteri speciali, come < e >, che possono essere usati per eseguire codice JavaScript non autorizzato. La sanitizzazione garantisce che i dati inseriti non vengano trattati come codice eseguibile.
- **Content Security Policy (CSP):** Implementare una rigorosa politica di sicurezza che controlli quali risorse (script, immagini, fogli di stile) possono essere caricate ed eseguite dal browser. La CSP limita le possibilità di iniezione di codice maligno.
- ***Sanitizzazione dell'output:*** Quando i dati forniti dall'utente vengono visualizzati sul sito web, è essenziale pulirli adeguatamente. Questo processo previene la possibilità che un utente malintenzionato possa sfruttare l'output per iniettare e far eseguire codice dannoso.

2. Miglioramenti strutturali: Architettura di rete

- ***Firewall applicativi (WAF):*** Il Web Application Firewall filtra e monitora il traffico HTTP tra utenti e applicazioni web, bloccando eventuali attacchi sospetti come SQLi, XSS e DDoS. È un importante strumento di difesa che agisce come una prima linea di protezione contro molteplici minacce.
- ***Logging e monitoring in tempo reale:*** L'implementazione di sistemi di log e monitoraggio permette di rilevare rapidamente anomalie nel traffico di rete o nei comportamenti degli utenti. Con il monitoraggio in tempo reale, è possibile reagire immediatamente a tentativi di attacco, riducendo i tempi di risposta e minimizzando i danni.
- ***Vantaggi dell'uso del cloud:***
- ***Ridondanza e scalabilità:*** I sistemi basati su cloud offrono maggiore flessibilità in termini di crescita e disponibilità. I log e i dati possono essere duplicati e conservati in più località, garantendo che non si perda nulla in caso di guasto.
- ***Accesso remoto:*** I team di sicurezza possono accedere ai log e ai dati da qualsiasi parte del mondo, senza la necessità di essere fisicamente connessi alla rete interna dell'azienda. Questo facilita un monitoraggio costante anche in caso di emergenze.

3. Sicurezza aziendale: Protezione contro attacchi DDoS

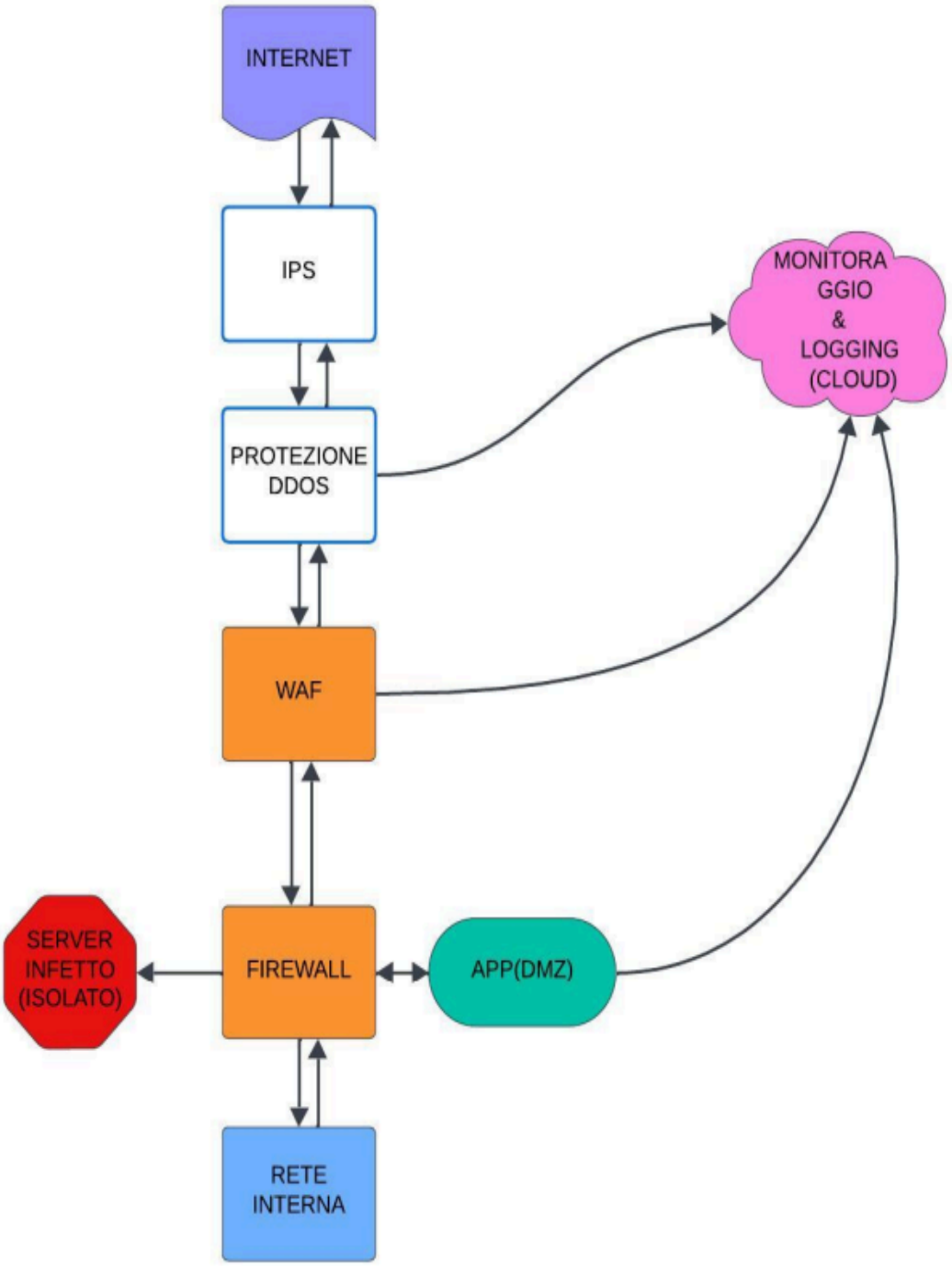
- ***Impatti finanziari di un attacco DDoS:***
- Un attacco DDoS può rendere un'applicazione web o un sito inaccessibile, causando perdite finanziarie immediate. Ad esempio, se un sito web subisce un downtime di **10 minuti**, con una stima di perdita di **1.500 € al minuto**, l'impatto totale sull'azienda potrebbe raggiungere i **15.000 €** solo per quei minuti di inattività.
- Oltre alla perdita diretta, si deve considerare anche il danno alla reputazione dell'azienda e la possibile perdita di fiducia da parte dei clienti.
- ***Azioni preventive:***
- ***Implementazione di un WAF con mitigazione DDoS:*** Questo sistema aiuta a bloccare tentativi di sovraccaricare i server con traffico malevolo, proteggendo l'infrastruttura dall'essere sovrastata da richieste dannose.
- ***Utilizzo di un Content Delivery Network (CDN):*** I CDN distribuiscono il traffico su vari server in tutto il mondo, riducendo il carico su un singolo server e mitigando il rischio di sovraccarico durante un attacco DDoS. Inoltre, possono bloccare traffico sospetto prima che raggiunga l'applicazione.

4. Risposta a incidenti: Malware

- ***Azioni immediate:***
- ***Isolamento del server infetto***: Non appena viene rilevata un'infezione da malware, il server compromesso deve essere isolato dal resto della rete per evitare la propagazione del codice malevolo. Questo può essere fatto mediante regole del firewall.
- ***Segmentazione della rete:*** Implementare VLAN o firewall interni permette di separare le varie porzioni della rete, limitando il danno potenziale in caso di infezione.
- Monitoraggio continuo: Continuare a osservare le attività del server infetto può fornire informazioni vitali sulle tecniche e sugli obiettivi dell'attaccante, permettendo di pianificare una risposta più efficace.

Strumenti consigliati:

- ***Intrusion Prevention System (IPS):*** Questo sistema identifica e blocca comportamenti sospetti in tempo reale, fermando le minacce prima che possano causare danni significativi.


INTERNET
IPS
MONITORA
GGIO
&
LOGGING
(CLOUD)
PROTEZIONE
DDOS
WAF
SERVER
INFETTO
(ISOLATO)
FIREWALL
APP(DMZ)
RETE
INTERNA

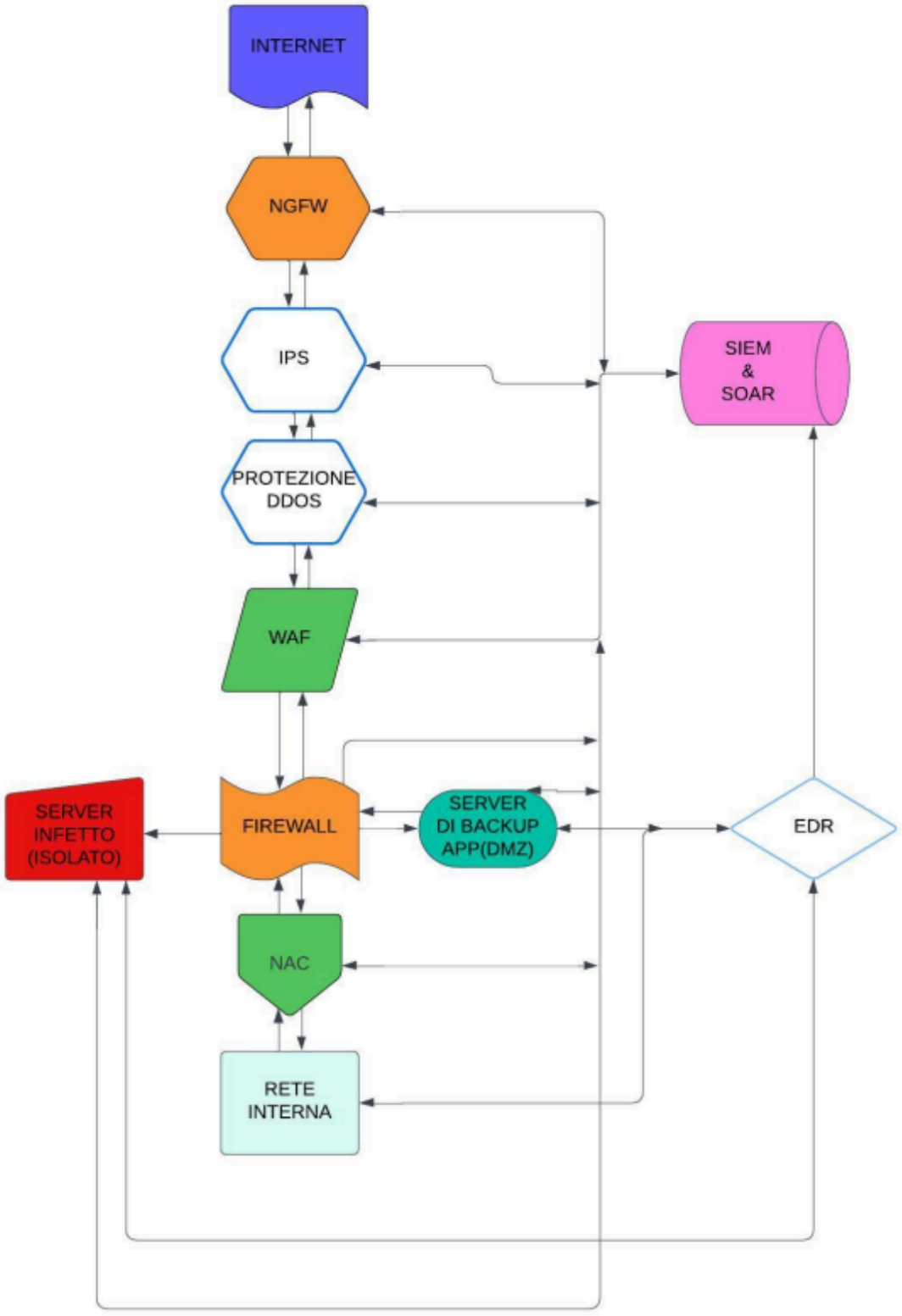
5. Soluzione integrata per la sicurezza

- La sicurezza non può essere garantita da una sola misura. È essenziale combinare diverse soluzioni preventive per proteggere efficacemente l'infrastruttura. Ciò include l'uso di firewall applicativi (WAF), mitigazione DDoS, monitoraggio continuo e strumenti IPS.
- ***Modifiche infrastrutturali:*** Potrebbe essere necessario apportare modifiche strutturali all'infrastruttura, come l'implementazione di regole di firewall più restrittive o l'uso di tecnologie di segmentazione della rete per isolare le porzioni critiche dell'infrastruttura.

6. Potenziamento dell'architettura di rete

Aggiunta di sistemi di sicurezza avanzati:

- ***Intrusion Prevention System (IPS)***: Integrare un IPS garantisce una protezione proattiva contro intrusioni e attacchi.
- ***Disaster Recovery Plan:*** Avere un piano di disaster recovery solido permette di riprendere rapidamente le attività in caso di downtime prolungato causato da attacchi o malfunzionamenti.
- ***Backup e Ripristino:*** Effettuare backup regolari e testare periodicamente i processi di ripristino garantisce che, in caso di attacco o perdita di dati, si possa ripristinare l'operatività in tempi rapidi.
- ***Server di emergenza:*** Implementare un server di backup di emergenza assicura che le operazioni critiche possano continuare anche in caso di compromissione del server principale.
- ***Network Access Control (NAC):*** Questo sistema controlla l'accesso alla rete basandosi su regole di sicurezza predefinite, garantendo che solo dispositivi conformi e autorizzati possano accedere alla rete aziendale. In caso contrario, il NAC può limitare o isolare il dispositivo in una rete di quarantena.
- ***Firewall di nuova generazione (NGFW):*** Questi firewall avanzati permettono una deep packet inspection (DPI), analizzando il contenuto dei pacchetti di rete a livello più profondo, permettendo il rilevamento di minacce come malware o tentativi di exploit nascosti nel traffico legittimo.
- ***SIEM & SOAR:***
- ***SIEM (Security Information and Event Management):*** Raccoglie, analizza e correla log e eventi di sicurezza, fornendo una visione centralizzata degli incidenti e aiutando a identificare anomalie o minacce.
- ***SOAR (Security Orchestration, Automation, and Response):*** Automatizza le risposte agli incidenti basandosi sui dati del SIEM, facilitando la gestione delle minacce in modo automatico o semi-automatico.
- ***EDR (Endpoint Detection and Response):*** Soluzione specializzata nel monitoraggio e nella protezione degli endpoint, rilevando e bloccando minacce come malware e ransomware.
- ***Architettura aggiornata aggressiva:*** Implementare NGFW, IPS, protezione DDoS, firewall applicativi, server di backup online, isolamento dei server compromessi e integrazione con sistemi NAC, SIEM, SOAR ed EDR.


INTERNET
NGFW
IPS
SIEM
&
SOAR
PROTEZIONE
DDOS
WAF
SERVER
INFETTO
(ISOLATO)
FIREWALL
SERVER
DI BACKUP
APP(DMZ)
EDR
NAC
RETE
INTERNA