W20D4 Benchmark

Azioni Preventive

Per difendere l'applicazione Web da attacchi di tipo SQLi (SQL Injection) e XSS (Cross-Site Scripting), si potrebbero implementare le seguenti azioni preventive:

- **Validazione degli Input**: Implementare la validazione e la sanitizzazione degli input degli utenti per prevenire SQLi e XSS.
- **Uso di Prepared Statements**: Utilizzare le dichiarazioni preparate nelle query SQL per prevenire l'iniezione di codice.
- **Content Security Policy (CSP)**: Implementare una politica di sicurezza dei contenuti per prevenire l'esecuzione di script non autorizzati.
- **Firewalls e Web Application Firewalls (WAF)**: Utilizzare firewall specifici per applicazioni web per monitorare e filtrare il traffico malevolo.

Modifica del Diagramma: possiamo aggiungere un Web Application Firewall (WAF) tra il Firewall e l'E-Commerce (DMZ) per evidenziare l'implementazione della sicurezza.

Impatti sul Business

Se l'applicazione Web subisce un attacco DDoS che la rende non raggiungibile per 10 minuti, l'impatto sul business può essere calcolato come segue:

- **Spesa media al minuto**: 1.500 €
- **Tempo di inattività**: 10 minuti
- **Impatto totale**: 1.500 €×10 minuti=15.000

Azioni preventive:

- **Limitare la larghezza di banda**: Implementare misure di limitazione della larghezza di banda per ridurre l'impatto degli attacchi DDoS.
- **Servizi di Mitigazione DDoS**: Utilizzare servizi di mitigazione DDoS per monitorare e proteggere l'infrastruttura.

Modifica del Diagramma: Si può aggiungere un'icona che rappresenta un servizio di mitigazione DDoS tra Internet e il Firewall.

Response al Malware

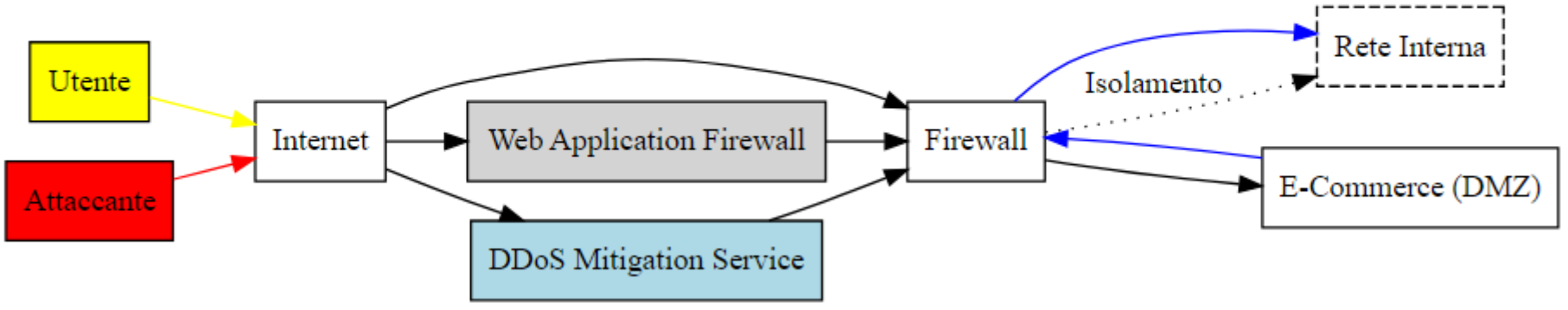
In caso di infezione da malware, la priorità è impedire che il malware si propaghi nella rete interna.

Azioni suggerite:

- **Isolamento del sistema infetto**: Implementare segmentazione della rete per isolare il sistema infetto.
- **Monitoraggio del traffico**: Aggiungere monitoraggio del traffico per rilevare comportamenti anomali.

Modifica del Diagramma: Si può aggiungere una connessione isolata tra il sistema infetto e la rete interna.

Soluzione Completa



Per implementare una **soluzione più aggressiva** per l'architettura di rete, potremmo considerare delle modifiche strutturali che migliorino la sicurezza, la resilienza agli attacchi e la protezione dell'infrastruttura. Queste modifiche potrebbero includere l'introduzione di un **Load Balancer**, una **segmentazione della rete più stretta** e l'aggiunta di **sistemi di backup e ripristino** per garantire la continuità operativa.

Modifica aggressiva

1. **Load Balancer**: Aggiungiamo un **Load Balancer** tra Internet e il Firewall. Il Load Balancer distribuisce il traffico tra più server, migliorando la resilienza agli attacchi DDoS e aumentando la disponibilità.
2. **Segmentazione della Rete**: Implementiamo una segmentazione più forte tra la **DMZ** e la **Rete Interna**. La DMZ viene ulteriormente isolata, limitando il traffico tra la DMZ e la rete interna.
3. **Sistemi di Backup e Ripristino**: Aggiungiamo un sistema di **backup e ripristino** per garantire che, in caso di attacco o disastro, sia possibile ripristinare rapidamente i servizi.