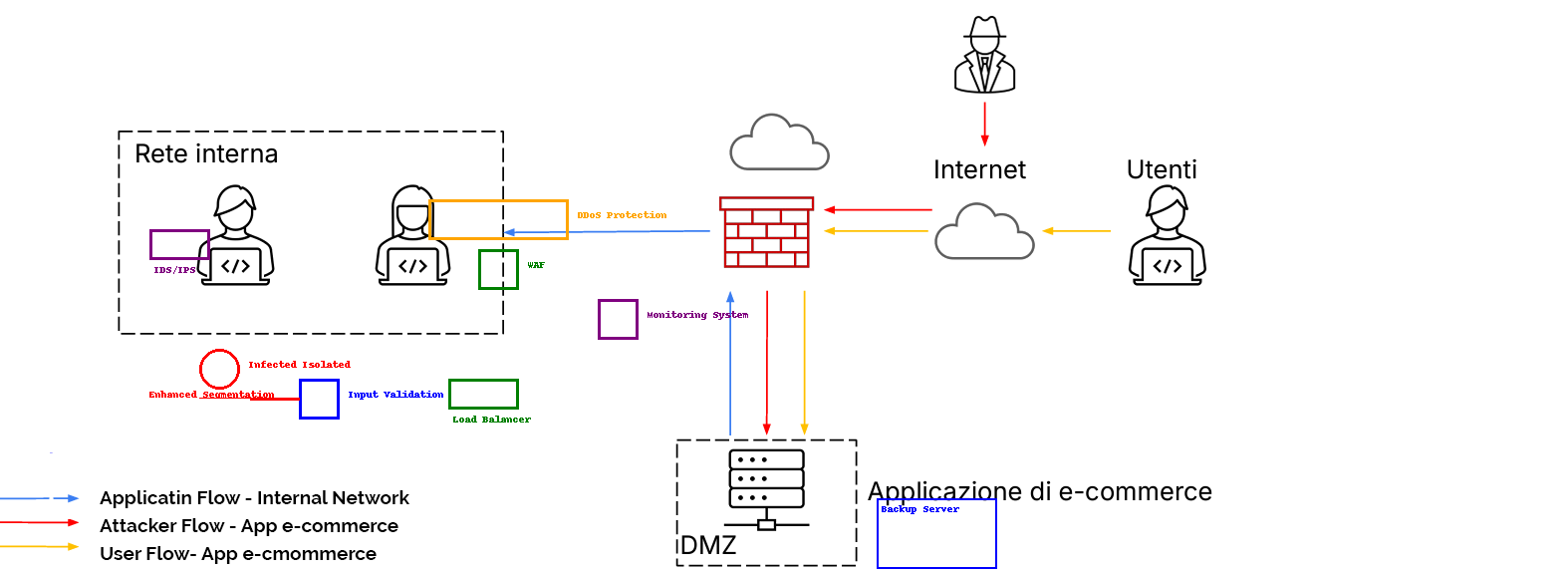
****

**1. Preventive Actions**

**Objective: Protect the web application from SQL Injection (SQLi) and Cross-Site Scripting (XSS) attacks.**

**Proposed Actions:**

* **Web Application Firewall (WAF): Deploy a WAF to filter and monitor HTTP traffic, blocking malicious requests attempting SQL Injection or XSS attacks.**
* **Input Validation and Sanitization:**
  + **Validate user inputs on both client and server sides.**
  + **Use parameterized queries or prepared statements in the database to prevent SQL Injection.**
  + **Escape or encode user inputs to avoid injecting malicious scripts, mitigating XSS attacks.**
* **Content Security Policy (CSP): Define allowed sources for scripts using a CSP to prevent unauthorized script execution.**
* **Encryption and Secure Communication: Enable HTTPS across all communication channels to prevent man-in-the-middle attacks and ensure secure communication.**

**2. Business Impact**

**Scenario: The web application suffers a DDoS attack, rendering it unavailable for 10 minutes.**

**Impact Assessment:**

* **Financial Loss:**
  + **Users spend an average of €1,500 per minute.**
  + **Total loss for 10 minutes of downtime: €15,000.**

**Preventive Actions:**

* **DDoS Protection Services: Use cloud-based DDoS mitigation services (e.g., Cloudflare, AWS Shield) to absorb and handle large-scale DDoS attacks.**
* **Rate Limiting: Configure rate-limiting rules to restrict the number of requests per IP address, reducing the effectiveness of bot-based attacks.**
* **Traffic Filtering: Use IP reputation databases and geo-blocking to filter traffic from known malicious regions or sources.**

**3. Response**

**Scenario: The web application is infected with malware.**

**Response Actions:**

* **Isolate the Infected Server: Disconnect the infected server in the DMZ from the internal network and the internet to prevent malware propagation.**
* **Forensic Analysis: Analyze system logs and malware behavior to identify the source of the infection and its impact.**
* **Remove Malware: Perform malware removal, sanitize the affected server, and ensure it is free of infection before reintegration.**
* **Patching and Updates: Update all systems with the latest security patches to prevent further exploitation.**

**4. Complete Solution**

**Objective: Integrate preventive actions and response measures to ensure comprehensive protection and quick recovery.**

**Implementation:**

* **Proactive Defenses:**
  + **Deploy WAF, input validation, CSP, and HTTPS to mitigate SQL Injection, XSS, and unauthorized traffic.**
* **Reactive Measures:**
  + **Implement malware isolation, forensic analysis, and sanitized recovery protocols to address incidents effectively.**
* **Business Continuity:**
  + **Establish redundancy mechanisms, including failover servers and robust backup systems.**

**5. Aggressive Infrastructure Modification**

**Objective: Enhance the security infrastructure with advanced capabilities for resilience and proactive protection.**

**Proposed Actions:**

* **Redundancy and Load Balancing: Deploy a load balancer to distribute traffic and maintain system availability during DDoS attacks or high traffic periods.**
* **Advanced Threat Detection: Introduce an Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) within the DMZ to detect and block malicious activities.**
* **Backup System: Implement a dedicated backup web server in a separate network segment to ensure business continuity during server downtime or malware isolation.**

**Conclusion:  
This incident response plan outlines comprehensive preventive and reactive measures to secure the e-commerce platform against cyber threats. By integrating WAF, input validation, CSP, encryption, DDoS mitigation, malware isolation, and advanced monitoring systems, the architecture achieves robust protection and ensures uninterrupted business operations.**