Project and report on security operations

1. Preventive Actions against SQL Injection and Cross-Site Scripting (XSS)

Preventive Actions:

- **Input Sanitization**: Use functions to escape and validate user input.
- **Prepared Statements**: Use parameterized queries to prevent SQL injection.
- **Web Application Firewall (WAF)**: Deploy a WAF to filter out malicious requests.
- **Content Security Policy (CSP)**: Configure CSP to prevent the execution of malicious scripts.
- **Secure Libraries and Frameworks**: Use secure validation libraries and keep software updated.

2. Business Impact of a DDoS Attack

Calculation of Impact:

- **Duration of Attack**: 10 minutes
- **Revenue Lost per Minute**: €1,500
- **Total Impact**: 10 minutes * €1,500/minute = €15,000

Preventive Actions:

- **DDoS Mitigation Service**: Use cloud-based services to absorb and mitigate DDoS traffic.
- **Load Balancer**: Distribute traffic across multiple servers to reduce the impact on a single server.
- **Redundancy and Failover**: Have backup servers ready to take over in case of an attack.

3. Response: Web Application Infected by Malware

Priority: Prevent Malware Propagation

- **Network Segmentation**: Isolate the infected machine by segmenting the network.
- **Continuous Monitoring**: Implement a monitoring system to detect lateral movements.
- **Communication Restrictions**: Limit the communications of the infected machine to only necessary ones for analysis.

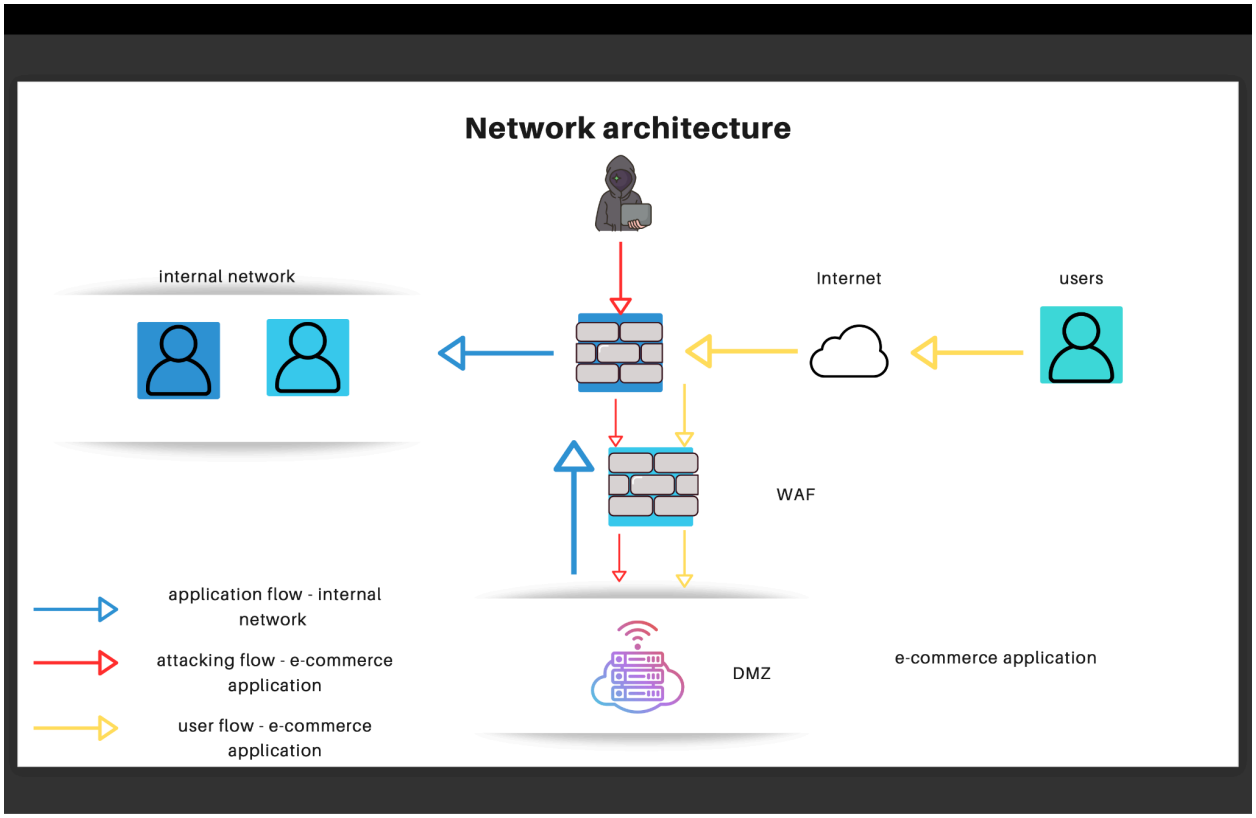
4. Comprehensive Solution: Combining Preventive and Response Actions

- **Input Sanitization, Prepared Statements, WAF, CSP**
- **Network Segmentation and Isolation**
- **Continuous Monitoring and Communication Restrictions**
-

5. Aggressive Infrastructure Modification (Integrating Solution for Point 2)

Additional Actions:

- **Regular Backups and Disaster Recovery Plans**: Implement strategies for regular backups and recovery plans.
- **Employee Training and Awareness**: Educate employees on security practices and threat recognition.
- **Penetration Testing**: Conduct periodic penetration testing to identify and fix vulnerabilities.
- **Regular System Updates**: Ensure all software is updated with the latest security patches.



Explanation

- **Input Sanitization and Validation**: All user inputs are sanitized and validated before being processed by the application.
- **Prepared Statements**: Used to prevent SQL injection.
- **WAF and CSP**: Protection against web attacks such as SQLi and XSS.
- **Network Segmentation**: Isolate infected machines to prevent malware propagation.
- **Load Balancer and DDoS Mitigation**: Defense against DDoS attacks.
- **Continuous Monitoring and Testing**: Detection and correction of vulnerabilities.
- **Regular Backups and Training**: Preparation for quick and effective incident responses.