# Cybersecurity Incident Report

## Network Attack Analysis

**Identification of the type of attack that caused the network interruption**

The malfunction of the website occurred due to a distributed denial of service (DDoS) attack. The attack flooded the web server with a large volume of forged SYN requests from multiple unknown IP addresses. This SYN traffic overload prevented the web server from processing legitimate user requests, resulting in connection timeout errors. The attack impacted the website's availability, negatively affecting user experience and the organization's business operations.

**Causes of website malfunction due to DDoS attack**

The malfunction of the website occurred due to a distributed denial of service (DDoS) attack. The attack flooded the web server with a large volume of forged SYN requests from multiple unknown IP addresses. This SYN traffic overload prevented the web server from processing legitimate user requests, resulting in connection timeout errors. The attack impacted the website's availability, negatively affecting user experience and the organization's business operations.

**Recommendations and Solutions**

To protect the network and prevent future attacks of this nature, several measures can be taken. Here are some suggestions:

1. **Implement an Intrusion Detection and Prevention System (IDPS)** to monitor network traffic and detect abnormal SYN traffic patterns.
2. **Configure limits and access controls to prevent server overload**, such as limiting the number of TCP SYN connections that can be established from an IP address within a specified time period.
3**. Use a DDoS mitigation system** that can identify and filter malicious traffic before it reaches the web server.
4**. Establish an incident response plan** that includes procedures for handling DDoS attacks and swiftly restoring web server functionality.
5. **Keep software and systems up to date** with the latest security patches to prevent known vulnerabilities that can be exploited in DDoS attacks.

6. **Packet Filtering**: Configure the company's firewall to filter and block SYN requests coming from suspicious or unknown IP addresses.
7. **Anomaly Detection**: Use anomaly detection systems to monitor network traffic and detect unusual behavior patterns that may indicate a DDoS attack.
8. **Cloud-based Attack Mitigation**: Consider using cloud-based attack mitigation services that can help filter malicious traffic before it reaches the web server.
9. **Load Balancing:** Implement load balancing solutions to evenly distribute traffic among multiple servers, helping mitigate the effects of a DDoS attack by not overwhelming a single server.
10. **System Updating and Patching**: Keep systems and applications up to date with the latest security patches to prevent vulnerabilities that could be exploited in a DDoS attack.

These measures can help protect the organization's network against future DDoS attacks and ensure the availability and proper functioning of the website.