CYBERSECURITY INCIDENT REPORT

Summary of the Incident:

On 21/6/25, the company's website became inaccessible to employees and customers due to a suspected cyberattack. After receiving a system alert and investigating the issue, I discovered the server was being overwhelmed by a large number of TCP SYN requests from an unfamiliar IP address. This pattern indicated a **SYN flood denial-of-service (DoS) attack**. As an immediate response, I took the web server offline to allow recovery and blocked the suspicious IP address via the firewall.

Analysis of the Attack:

I used a packet sniffer to analyze traffic to and from the company's web server and found a flood of incomplete TCP connections. A single IP address was sending a high volume of **TCP SYN packets** without completing the full handshake process (SYN-ACK-ACK). This behavior suggests its a **SYN flood attack**, a type of **DoS (Denial of Service)** attack.

In a SYN flood, the attacker sends many connection requests (SYNs) but never completes the handshake. The server allocates resources for each connection and eventually becomes overwhelmed, causing it to stop responding to legitimate traffic, which is alarming.

As a result, our website was unable to load, generating timeout errors for users. Employees couldn't access the sales page, which disrupted customer service and internal operations. If unaddressed, this attack could lead to **revenue loss, damaged customer trust**, and **reputational harm**.

I temporarily blocked the attacking IP address via the firewall. However, since attackers can use **IP spoofing**, this is not a long-term solution.

Recommendations:

1. **Enable SYN cookies** on the server to prevent resource exhaustion from half-open connections.
2. **Implement rate limiting** to restrict the number of requests from a single IP address.
3. **Use a Web Application Firewall (WAF)** to detect and block abnormal traffic patterns.
4. **Monitor traffic** continuously with intrusion detection/prevention systems (IDS/IPS).
5. **Consider a cloud-based DDoS protection service** like Cloudflare or AWS Shield for future resilience.