**INCIDENT REPORT ANALYSIS**

|  |  |
| --- | --- |
| Summary | This afternoon, the company experienced a distributed denial-of-service (DDoS) attack that disrupted the internal network for two hours. Network services suddenly stopped responding due to a flood of incoming ICMP packets. Normal internal traffic was unable to access any network resources. The incident response team identified that the malicious actor exploited a misconfigured firewall, which allowed unlimited ICMP traffic into the network. During the attack, critical services were unavailable, causing interruptions to employee productivity and client communications. |
| Identify | The incident management team audited the firewall configuration, network services, and monitoring tools involved in the attack. The team discovered that the firewall had not been configured to filter or limit ICMP packets, allowing the attacker to overload the company’s internal network. As a result, employees were unable to access internal services for two hours. |
| Protect | The team implemented new firewall rules to restrict the rate of incoming ICMP traffic and verify the source IP addresses to prevent spoofing. In addition, nonessential services were temporarily taken offline to reduce system load. Moving forward, the company will provide staff with training on secure firewall configurations and update security policies for network infrastructure. |
| Detect | To improve detection of future attacks, the team deployed network monitoring software to identify abnormal traffic patterns and installed an intrusion detection and prevention system (IDS/IPS). Automated alerts have been configured to notify the security team of suspicious ICMP traffic in real time. |
| Respond | The team blocked the incoming ICMP traffic and restored essential network services first to minimize business disruption. Logs were reviewed to analyze the traffic source and attack method. A post-incident meeting with management has been scheduled to discuss lessons learned, and the security team is updating the incident response plan to include DDoS-specific procedures. |
| Recover | The company’s internal network was restored to full functionality within two hours of the attack. System integrity checks confirmed that no permanent data loss occurred. A post-incident review has been initiated, and baseline configurations have been updated to prevent recurrence. The company will also explore disaster recovery (DR) enhancements to reduce downtime in the event of future large-scale attacks. |

|  |  |
| --- | --- |
| Reflections/note | This incident highlighted the critical importance of proper firewall configuration. A small oversight left the company vulnerable to a large-scale attack.  Proactive monitoring tools such as IDS/IPS and anomaly detection could have provided earlier warning and reduced downtime.  The need for a comprehensive incident response plan (IRP) specific to DDoS attacks is clear; response was effective but could be faster with rehearsed playbooks.  Staff training and ongoing security awareness are vital to ensure all employees and administrators understand how configuration and policy gaps create risks.  Future investment in redundancy and disaster recovery strategies will help minimize operational impact in case of similar attacks. |