**Incident report analysis**

|  |  |
| --- | --- |
| **Summary** | The company experienced a significant security incident characterized by a distributed denial of service (DDoS) attack targeting network services. The attack, initiated through a flood of ICMP packets, led to a disruption in all network services, prompting the cybersecurity team to swiftly respond by halting non-critical services to prioritize the restoration of critical network functionalities. |
| Identify | The cybersecurity team identified that malicious actors executed an ICMP flood attack, impacting the entire internal network. Critical network resources were compromised, necessitating immediate action to secure and restore them to normal operation. |
| Protect | In response to the incident, the following protective measures were implemented:   * **Firewall Rule Enhancement:** Implemented a new firewall rule to restrict the rate of incoming ICMP packets, mitigating the impact of future ICMP flood attacks. * **Intrusion Detection/Prevention Systems (IDS/IPS):** Deployed IDS/IPS systems to filter out suspicious ICMP traffic, enhancing network defence capabilities. |
| Detect | To enhance detection capabilities and monitor for anomalous network behaviour, the following measures were implemented:   * **Source IP Address Verification:** Configured on the firewall to detect and block spoofed IP addresses associated with incoming ICMP packets. * **Network Monitoring Software:** Implemented to continuously monitor network traffic patterns and identify abnormal activity indicative of potential attacks. |
| Respond | Immediate response actions included:   * **Isolation of Affected Systems:** Isolated compromised network segments to contain the spread of the DDoS attack and prevent further disruption. * **Restoration of Critical Services:** Prioritized the restoration of critical network services to minimize downtime and mitigate operational impact. * **Incident Reporting:** Reported the incident to upper management and relevant legal authorities to ensure compliance with regulatory requirements and facilitate further investigation. |
| Recover | Efforts to recover from the DDoS attack included:   * **Service Restoration:** Restored network services to their normal functioning state by halting non-critical services initially and gradually reintroducing them post-attack. * **Post-Incident Analysis:** Analysed network logs and traffic patterns to identify the attack vectors and strengthen defences against future DDoS attacks. * **Preventive Measures:** Enhanced firewall configurations and implemented proactive measures to block external ICMP flood attacks in the future. |

|  |  |
| --- | --- |
| Recommendation | 1. **Regular Security Audits:** Conduct routine audits of network infrastructure and security controls to identify vulnerabilities and gaps. 2. **Employee Training:** Continuously educate employees on cybersecurity best practices, including recognizing and reporting suspicious activities. 3. **Incident Response Planning:** Develop and test comprehensive incident response plans to ensure swift and effective responses to cyber incidents. 4. **Backup and Recovery:** Strengthen backup protocols to ensure timely data recovery and minimize data loss in the event of a security breach. |

|  |  |
| --- | --- |
| Conclusion | While the DDoS attack posed significant challenges, the prompt and coordinated response by the cybersecurity team mitigated potential damage and facilitated the restoration of critical network services. Moving forward, ongoing vigilance, proactive security measures, and continuous improvement in cybersecurity practices will be paramount to safeguarding the company's network infrastructure against evolving threats. |