**Incident report analysis**

|  |  |
| --- | --- |
| **Summary** | The company experienced a security event when all network services suddenly stopped responding. The cybersecurity team found the disruption was caused by a distributed denial of services (DDoS) attack through a flood of incoming ICMP packets. The team responded by blocking the attack and stopping all non-critical network services, so that critical network services could be restored. |
| Identify | The team has implemented new authentication policies to prevent future attacks: multi-factor authentication (MFA), login attempts limited to three tries, and training for all employees on how to protect login credentials. Additionally, we will implement a new protective firewall configuration and invest in an intrusion prevention system (IPS). |
| Protect | To protect against future DDoS attacks, the organization can implement measures such as network segmentation, firewall rules, and Intrusion detection systems. By implementing these protections, the impact of future attacks can be minimized or prevented. |
| Detect | The incident management team should have mechanisms in place to detect any potential DDoS attacks, such as monitoring network traffic patterns, analyzing logs and systems alerts. Intrusion detection systems and real time network monitoring can help identify any abnormal traffic patterns associated with DDoS attacks. |
| Respond | In response to the DDoS attack, the incident management team promptly responded by blocking incoming ICMP packets at the network perimeter, isolating the attack and preventing further disruption. They also resolved the attack within two hours. This quick response helps minimize the impact and restore normal network services. |
| Recover | After the attack is resolved, the organization should assess the damage caused, restore services, and investigate any potential data loss or compromise. This includes conducting a post incident analysis to identify the source, motive, potential vulnerabilities exploited. Any necessary actions can then be taken to prevent future attacks. |

|  |
| --- |
| Reflections/Notes: After the incident, it is important to continuously improve the organization’s cybersecurity posture. This can involve conducting regular vulnerability assessments, penetration testing, and updating security policies and procedures. By continuously reviewing and improving security measures, the organization can adapt to emerging threats and strengthen their overall cybersecurity capabilities.  Finally, the incident management team maintains open lines of communication with their internet service provider (ISP) to report any suspicious activity or request assistance in mitigating future DDoS attacks. This collaboration helps to ensure quick and effective response in case of any future incidents. |