Incident Report Analysis: Graphic Design Company

Summary:

The company experienced a significant security incident where all network services suddenly became unresponsive. The cybersecurity team determined that the disruption was caused by a distributed denial of service (DDoS) attack utilizing a flood of incoming ICMP packets. To mitigate the impact, the team took immediate action by blocking the attack and temporarily suspending non-critical network services, allowing them to focus on restoring critical network services.

Identification:

A targeted DDoS attack employing an ICMP flood affected the entire internal network, leading to the disruption of critical network resources. The primary objective was to secure and restore the affected network services to their normal functioning state.

Protection:

To enhance network security and protect against future attacks, the cybersecurity team implemented a new firewall rule to limit the rate of incoming ICMP packets. Additionally, an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) was deployed to filter out ICMP traffic exhibiting suspicious characteristics.

Detection:

To improve threat detection capabilities, the cybersecurity team implemented source IP address verification on the firewall, enabling the identification of spoofed IP addresses on incoming ICMP packets. Furthermore, network monitoring software was deployed to detect abnormal traffic patterns and promptly identify potential security incidents.

Response:

For future security events, the cybersecurity team has established a response plan. In the event of an incident, affected systems will be isolated to prevent further disruptions to the network. Critical systems and services impacted by the event will be prioritized for restoration. The team will conduct thorough analysis of network logs to identify any suspicious or abnormal activity. Additionally, all incidents will be reported to upper management and appropriate legal authorities, if necessary.

Recovery:

To recover from a DDoS attack involving ICMP flooding, the restoration of network services to a normal functioning state is crucial. In the future, external ICMP flood attacks can be effectively blocked at the firewall level. During the recovery process, non-critical network services should be temporarily halted to minimize internal network traffic. Critical network services should be restored first, followed by bringing non-critical systems and services back online after the flood of ICMP packets has subsided.