**Incident report analysis**

| **Summary** | My organization is a multimedia company that provides web design services, graphic design, and social media marketing solutions to small businesses. It has recently experienced a cybersecurity incident, which compromised the organization for two hours until it was resolved. During the attack, network services stopped responding because of a flood of ICMP packets. The incident management team responded by blocking incoming ICMP packets. | | |
| --- | --- | --- | --- |
| Identify | The cybersecurity team found out that a malicious actor or actors had sent a flood of ICMP packets to the organization’s unconfigured firewall. This vulnerability allowed the malicious attacker to perform a distributed denial of service (Ddos) attack on the company’s network. All critical networks needed to be secured and restored to its services. | | |
| Protect | To address this incident, the network security team implemented an immediate action plan, a firewall rule to limit the rate of incoming ICMP packets, installing an IDS/IPS system to filter out ICMP traffic based on suspicious characteristics. | | |
| Detect | To detect any unusual activity in the future, the security team configured the organization’s firewall for better network hardening to verify source IP address and detect IP spoofed addresses on incoming ICMP packets. The security team will also monitor network traffic by the use of SIEM tools to detect abnormal traffic patterns. | | |
| Respond | For future security incidents, the cybersecurity team will set up an immediate action plan to restore critical networks back to functional operation. Analyze network logs to check for abnormal activity, have an overview on where and how a malicious actor did an attack. The security team will also have a security incident report for upper management and legal authorities. | | |
| Recover | To recover from a Ddos attack by an ICMP flooding, the organization needs to proactively configure the company’s firewall and update regularly before an incident occurs. During an incident like a Ddos attack, access to network services needs to be restored to a normal functioning state, all non-critical networks should be stopped to reduce internal network traffic for better incident monitoring and pinpoint the source of the attack. Restoring all critical networks should be the first priority. Once the ICMP packets have timed out, only then all non-critical networks can be brought online. | | |