**Incident report analysis**

**Instructions**

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this chart as a way to practice applying the NIST framework to different situations you encounter.

|  |  |
| --- | --- |
| **Summary** | The organization’s networks services stopped responding, disrupting operations for 2 hours. Investigations revealed that a Distributed Denial of Service attack was launched and flooded the network with ICMP packets. The attack exploited an unconfigured firewall, allowing the malicious actor to overwhelm the network and prevent normal network traffic from accessing our resources.  The incident response team responded by blocking incoming ICMP packets, taking non-critical services offline, and restoring critical network services. The cybersecurity team investigated the situation and implemented several changes including new firewall rule to limit the rate of incoming ICMP packets, verifying source IP addresses to prevent spoofing, deploying network monitoring software to detect abnormal traffic and introducing IDS/IPS system to filter suspicious ICMP traffic. |
| Identify | The DDoS attack impacted on the organization’s firewall, network infrastructure and critical services. The attack began with a flood of ICMP packets entering through an unconfigured firewall, overwhelming the network and disrupting all internal network traffic and critical services for 2 hours. This affected internal communication, shared resource access and client services causing delays in operations. |
| Protect | The company’s cybersecurity team has implemented stricter access control measures such as limiting ICMP packet rates and verifying IP sources to block malicious traffic and ensure only trusted access. Employees need training on secure configurations and network monitoring and It staff should adopt stronger proactive measures. Sensitive data should always be encrypted and procedures such as firewall configurations should be monitored and updated regularly. The company also implemented Network monitoring tools to aid with identifying and blocking threats. |
| Detect | Continuous monitoring is essential, the company has implemented intrusion detection systems to analyze data packets entering the network and various network monitoring tools (e.g. SIEM tools like Splunk) to identify potential threats early and provide visibility into network traffic and detect unusual activities. |
| Respond | Clear action plans for isolating affected resources, restoring services and blocking malicious traffic should be made alongside communication procedures to keep IT staff, management and employees informed of the situation. The incident response team blocked off all incoming ICMP packets to reduce the attack’s impact. It will be important in the future to log and analyze traffic to identify attack sources and refine defenses. Law enforcement will be informed, and customers will be emailed to inform them of the incident that occurred. |
| Recover | To recover from this incident it is imperative that firewall configurations are regularly checked and updated to avoid unverified access. |

|  |
| --- |
| Reflections/Notes: |