NIST CSF Security Plan

Summary

During a DDoS attack, a multimedia organization's network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.

The company's cybersecurity team then investigated the security event. They found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company's network through a distributed denial of service (DDoS) attack.

To address this security event, the network security team implemented:

- A new firewall rule to limit the rate of incoming ICMP packets.
- Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets.
- Network monitoring software to detect abnormal traffic patterns.
- An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.

Identify

Security Risk Audits:

- Schedule routine checks of internal networks, systems, and devices to pinpoint potential vulnerabilities.
- Use vulnerability scanning tools to detect outdated software or potential weaknesses.
- Conduct penetration testing to simulate potential attacks and identify weak points.
- Regularly review user permissions to ensure that only the necessary individuals have access to sensitive data or systems.

System Inventory:

- Maintain an up-to-date list of all systems, devices, and software in use to aid in identifying potential gaps.

Incident Classification:

- The type of attack: DDoS via ICMP flood.
- Systems impacted: Internal network services.

Protect

Policies and Procedures:

- Establish, review, and update network security policies. This includes setting up and configuring firewalls, IDS/IPS, and other security measures.

- Develop and enforce policies on access controls, ensuring least privilege.

Training:

- Educate employees about the dangers of phishing, the importance of strong password policies, and the significance of keeping software updated.
- Technical training for IT and security staff on the latest threats and protection mechanisms.

Protection Plan:

- Ensuring firewalls are adequately configured to block unnecessary or malicious traffic.
- Implementing regular software updates and patches.
- Backing up critical data regularly.

Detect

Network Monitoring:

- Use the network monitoring software to detect and alert on unusual traffic patterns or spikes in real-time activity.
- Regularly review and analyze system and access logs to detect unauthorized or suspicious activities or anomalies.
- Configure source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets.

IDS/IPS:

- Make sure the Intrusion Detection/Prevention System is calibrated to identify and stop malicious ICMP traffic or any other suspicious patterns.

Alerts:

- Ensure timely notifications to the relevant teams in case of potential threats.
- Implement User and Entity Behavior Analytics (UEBA) to detect abnormal user activities.

Respond

Containment:

- Segment the network to isolate affected devices.
- Immediately block malicious IP addresses or domains.
- Disable affected ports or reroute traffic.

Neutralization:

- Have pre-configured firewall rules to quickly implement during an attack.
- Utilize the IDS/IPS system to block malicious patterns.

Incident Analysis:

- Analyze network logs, IDS/IPS alerts, and any other relevant data.
- Collaborate with external security experts or organizations for deeper insights.

Improvement:

- Based on the incident, refine response procedures.
- Regularly conduct drills or simulated attacks to practice the response process.

Recover

Restoration Plans:

- Develop a plan to restore systems to their normal state after an incident.
- For systems impacted by DDoS, this might include clearing the system cache, rebooting systems, or refreshing DNS servers.

Data Recovery:

- Regularly backup data and ensure a robust data recovery solution is in place.
- Test the recovery processes periodically to ensure they are effective.

Post-Incident Analysis:

- After recovery, conduct a thorough analysis of the incident. Determine what went well, what can be improved, and then iterate on the response and recovery plans.
- Implement a Disaster Recovery (DR) and Business Continuity Plan (BCP).

By incorporating the NIST CSF into the company's cybersecurity strategy, the organization will be better equipped to handle potential threats, ensuring a resilient and secure operational environment.