**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 recently experienced a DDoS attack which was due to a flood of ICMP packets. Normal internal traffic was unable to access any network resources. The incident team blocked all incoming ICMP packets and stopped all non-critical network services offline and restoring critical network services. |
| Identify | Through an audit the incident management team determined that the firewall had been configured incorrectly. This allowed the malicious attacker to overwhelm the company’s network. |
| Protect | The incident management team has introduced a new firewall rule to limit the rate of incoming ICMP packets. Security hardening to check for spoofed IP addresses on incoming ICMP packets. |
| Detect | To detect further intrusions an IDP/IPS system will be used to filter out ICMP traffic based on suspicious characteristics. As well as network monitoring software such as SIEM to detect abnormal traffic patterns. |
| Respond | The incident management team blocked incoming ICMP packets, stopped all non-critical network services offline and restored critical network services. We informed users of the breach. For future security events the cybersecurity team will isolate affected systems to prevent further disruption and attempt to restore any critical systems and services disrupted by the event. The team will then analyze network logs for abnormal activity and report all incidents to upper management and legal authorities, if applicable. |
| Recover | We restored the site to normal functionality after implementing new firewall configurations and source IP address verification. Also implemented new network monitoring software and IDS/IPS system. To recover from a DDoS attack by ICMP flooding, access to network services need to be restored to a normal functioning state. In the future, external ICMP flood attacks can be blocked at the firewall. Then, all non-critical network services should be stopped to reduce internal network traffic. Next, critical network services should be restored first. Finally, once the flood of ICMP packets have timed out, all non-critical network systems and services can be brought back online. |

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

**Incident report analysis**

**Instructions**

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

|  |  |
| --- | --- |
| **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 | A malicious actor or actors targeted the company with an ICMP flood attack. The entire internal network was affected. All critical network resources needed to be secured and restored to a functioning state. |
| Protect | The cybersecurity team implemented a new firewall rule to limit the rate of incoming ICMP packets and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics. |
| Detect | The cybersecurity team configured source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets and implemented network monitoring software to detect abnormal traffic patterns. |
| Respond | For future security events, the cybersecurity team will isolate affected systems to prevent further disruption to the network. They will attempt to restore any critical systems and services that were disrupted by the event. Then, the team will analyze network logs to check for suspicious and abnormal activity. The team will also report all incidents to upper management and appropriate legal authorities, if applicable. |
| Recover | To recover from a DDoS attack by ICMP flooding, access to network services need to be restored to a normal functioning state. In the future, external ICMP flood attacks can be blocked at the firewall. Then, all non-critical network services should be stopped to reduce internal network traffic. Next, critical network services should be |

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

**Incident report analysis - Example**

|  |  |
| --- | --- |
| **Summary** | This morning, an intern reported to the IT department that she was unable to log in to her internal network account. Access logs indicate that her account has been actively accessing records in the customer database, even though she is locked out of that account. The intern indicated that she received an email this morning asking her to go to an external website to log in with her internal network credentials to retrieve a message. We believe this is the method used by a malicious actor to gain access to our network and customer database. A couple of other employees have noticed that several customer records are either missing or contain incorrect data. It appears that not only was customer data exposed to a malicious actor, but that some data was deleted or manipulated as well. |
| Identify | The incident management team audited the systems, devices, and access policies involved in the attack to identify the gaps in security. The team found that an intern’s login and password were obtained by a malicious attacker and used to access data from our customer database. Upon initial review, it appears that some customer data was deleted from the database. |
| Protect | 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). |
| Detect | To detect new unauthorized access attacks in the future, the team will use a firewall logging tool and an intrusion detection system (IDS) to monitor all incoming traffic from the internet. |
| Respond | The team disabled the intern’s network account. We provided training to interns and employees on how to protect login credentials in the future. We informed upper management of this event and they will contact our customers by mail to inform them about the data breach. Management will also need to inform law enforcement and other organizations as required by local laws. |
| Recover | The team will recover the deleted data by restoring the database from last night’s full backup. We have informed staff that any customer information entered or changed this morning would not be recorded on the backup. So, they will need to re-enter that information into the database once it has been restored from last night’s backup. |

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

**Applying the NIST CSF**

Earlier in this program you learned about the uses and benefits of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). There are five core functions of the NIST CSF framework: identify, protect, detect, respond, and recover.

A diagram of a process

Description automatically generated

*Image: 5 core functions of the NIST CSF*

These core functions help organizations manage cybersecurity risks, implement risk management strategies, and learn from previous mistakes. Plans based on this framework should be continuously updated to stay ahead of the latest security threats. The core functions help ensure organizations are protected against potential threats, risks, and vulnerabilities. Each function can be used to improve an organization’s security:

* **Identify:** Manage security risks through regular audits of internal networks, systems, devices, and access privileges to identify potential gaps in security.
* **Protect**: Develop a strategy to protect internal assets through the implementation of policies, procedures, training and tools that help mitigate cybersecurity threats.
* **Detect**: Scan for potential security incidents and improve monitoring capabilities to increase the speed and efficiency of detections.
* **Respond**: Ensure that the proper procedures are used to contain, neutralize and analyze security incidents and implement improvements to the security process.
* **Recover**: Return affected systems back to normal operation and restore systems data and assets that have been affected by an incident.

Some questions to ask for each of the five core functions, include:

|  |  |
| --- | --- |
| Identify | Create an inventory of organizational systems, processes, assets, data, people, and capabilities that need to be secured:   * Technology/Asset Management: Which hardware devices, operating systems, and software were affected? Trace the flow of the attack through the internal network. * Process/Business environment: Which business processes were affected in the attack? * People: Who needs access to the affected systems? |
| Protect | Develop and implement safeguards to protect the identified items and ensure delivery of services:   * Access control: Who needs access to the affected items? How are non-trusted sources blocked from having access? * Awareness/Training: Who needs to be made aware of this attack and how to prevent it from happening again? * Data security: Is there any affected data that needs to be made more secure? * Information protection and procedures: Do any procedures need to be updated or added to protect data assets? * Maintenance: Do any of the affected hardware, operating systems, or software need to be updated? * Protective technology: Are there any protective technologies, like a firewall or an intrusion prevention system (IDS), that should be implemented to protect against future attacks? |
| Detect | Design and implement a system with tools needed for detecting threats and attacks:   * Anomalies and events: What tools could be used to detect and alert IT security staff of anomalies and security events, such as a security information and event management system (SIEM) tool? * Security continuous monitoring: What tools or IT processes are needed to monitor the network for security events? * Detection process: What tools are needed to detect security events, such as an IDS? |
| Respond | Design action plans for responding to threats and attacks:   * Response planning: What action plans need to be implemented to respond to similar attacks in the future? * Communications: How will security event response procedures be communicated within the organization and with those directly affected by the attack, including end users and IT staff? * Analysis: What analysis steps should be followed in response to a similar attack? * Mitigation: What responding steps could be used to mitigate the impact of an attack, such as offlining or isolating affected resources? * Improvements: What improvements are needed to improve response procedures in the future? |
| Recover | Construct a plan and implement the framework for recovering and restoring affected systems and/or data:   * Recovery planning: How will resources be restored following an attack? * Improvements: Do any improvements need to be made to the current recovery systems or processes? * Communications: How will restoration procedures be communicated within the organization and with those directly affected by the attack, including end users and IT staff? |

The NIST CSF and its five core functions provide a framework of planning proactive to applying reactive measures to cybersecurity threats. These functions are essential for ensuring that an organization has effective security strategies in place. An organization must have the ability to quickly recover from any damage caused by an incident to minimize their level of risk.