**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 security incident involved a Distributed Denial of Service (DDoS) attack targeting our internal network. The attack was caused by a flood of ICMP packets exploiting an unconfigured firewall. This resulted in a complete disruption of network services for approximately two hours. In response, we immediately blocked incoming ICMP packets, halted non-critical network services to mitigate the attack's spread, and focused on restoring critical network functions promptly. The attack primarily targeted our internal network infrastructure and critical network services. The source of the attack was traced to a malicious actor using spoofed IP addresses, which posed challenges in identifying and blocking the origin. The estimated impact included a significant loss of network services for the duration of the incident, potentially leading to operational disruptions for our business services. |
| Identify | In identifying the impact and systems affected, our inventory highlighted several critical areas. The attack primarily affected internal network devices, including firewalls critical to our network security architecture. Business operations such as network services, web design, graphic design, and social media marketing solutions were severely disrupted. Regarding access control, only IT staff and network administrators require access to affected systems for diagnostics and resolution. |
| Protect | To safeguard against future incidents, we are implementing several protective measures. Access control measures will restrict access to critical network configurations and firewall settings exclusively to authorized personnel. Ongoing awareness and training initiatives will educate our IT staff and network administrators on identifying and mitigating DDoS attacks. Critical data will be fortified through regular encryption and comprehensive backup procedures. Updated incident response protocols and stringent maintenance schedules will ensure timely updates and patches for all hardware, operating systems, and software. Advanced protective technologies, including enhanced firewall configurations and IDS/IPS deployment, will further fortify our defenses against future attacks. |
| Detect | Our strategy for detecting potential cybersecurity incidents revolves around implementing robust threat detection systems. Leveraging a Security Information and Event Management (SIEM) tool will enable us to monitor and detect anomalies and security events promptly. Continuous network monitoring tools will actively scan for abnormal traffic patterns indicative of potential attacks. Furthermore, deploying an Intrusion Detection System (IDS) will enhance our capability to identify and respond to suspicious activities within our network infrastructure swiftly. |
| Respond | In response to cybersecurity threats and attacks, we have developed comprehensive action plans. These plans outline immediate responses and long-term strategies tailored to similar incidents in the future. Clear internal communication protocols have been established to facilitate seamless coordination among IT staff and end-users during response efforts. Our incident analysis and forensic investigation procedures are meticulously outlined to ensure thorough examination and data collection. Mitigation measures include isolating affected resources and restoring services swiftly to minimize operational disruptions. Continuous improvements to response procedures are prioritized based on insights gained from incident reviews and assessments. |
| Recover | Our recovery and restoration plan focuses on expeditiously restoring affected systems and services following a cybersecurity incident. We have developed detailed strategies for resource allocation and service restoration. Continuous enhancements to our recovery systems and processes are being implemented to streamline future recovery efforts. Clear communication protocols are in place to ensure transparent and timely updates regarding restoration procedures to IT staff and end-users. |

|  |
| --- |
| Reflections/Notes:  Throughout this incident response analysis, we've identified key areas where our cybersecurity posture can be strengthened. Enhancements in access control, such as stricter firewall rules and access management policies, will fortify our defenses against unauthorized access and potential future attacks. Regular training and awareness programs will empower our team to proactively identify and respond to emerging threats effectively. Strengthening our detection capabilities with advanced monitoring tools and real-time threat intelligence will enable us to detect and mitigate threats more swiftly. Additionally, refining our response and recovery plans based on lessons learned from this incident will ensure we are better prepared to handle future cybersecurity challenges. Continuous reflection and adaptation are essential to maintaining a resilient cybersecurity framework in our organization. |