Oksana Syvun

Incident report analysis

Summary	The scenario involves a multimedia company that offers web design, graphic design, and social media marketing services to small businesses. The company experienced a DDoS attack, which compromised the internal network for two hours until it was resolved. The attack was caused by a flood of ICMP pings sent through an unconfigured firewall, which overwhelmed the company's network.
Identify	Based on the scenario, the type of attack that occurred was a distributed denial of service (DDoS) attack. This type of attack aims to overwhelm a network or website by flooding it with traffic from multiple sources, thereby making it unavailable to users.
Protect	Based on the scenario, the following systems or procedures can be updated or changed to further secure the organization's assets: **Configuration of Firewalls**: The firewall configuration can be reviewed and updated to block all incoming ICMP packets and prevent the possibility of DDoS attacks in the future. Also, the firewall can be configured to check for spoofed IP addresses on incoming ICMP packets, which will help mitigate the possibility of malicious traffic. **Regular Audits**: Regular audits of internal networks, systems, devices, and access privileges can be conducted to identify potential gaps in security and address them before they are exploited. **Network Monitoring**: Network monitoring software can be deployed to detect abnormal traffic patterns and speed up the detection of potential security incidents. **Security Training and Awareness**: Training and awareness programs can be established to educate employees about the importance of security and provide guidelines for secure use of the network and devices. This can help prevent security incidents caused by human error or negligence.

	By implementing these changes, the organization can improve its security posture and reduce the likelihood of similar incidents occurring in the future.
Detect	There are several ways that security teams can monitor and analyze network traffic, software applications, track authorized versus unauthorized users, and detect any unusual activity on user accounts. Here are a few examples: **Network Monitoring**: Security teams can monitor network traffic using network security tools such as firewalls, intrusion detection and prevention systems (IDS/IPS), and network traffic analysis (NTA) solutions. These tools can be used to detect and analyze incoming and outgoing traffic, identify suspicious behavior and patterns, and prevent unauthorized access. **Application Monitoring**: Security teams can monitor software applications for vulnerabilities, errors, and malicious activity using application performance monitoring (APM) tools. These tools can help identify and resolve issues that could be exploited by attackers. **User Activity Monitoring**: Security teams can monitor user activity by implementing user activity monitoring (UAM) solutions. These tools can be used to track user activity, detect anomalies, and alert security teams to potential threats. **Identity and Access Management**: Security teams can use identity and access management (IAM) solutions to track authorized versus unauthorized users. IAM tools can help manage user access to systems and data, enforce security policies, and provide visibility into user activity. **Security Information and Event Management**: Security teams can use security information and event management (SIEM) tools to collect, analyze, and correlate security events across the organization. SIEM tools can help detect security incidents, investigate incidents, and provide real-time alerts to security teams. By implementing these and other monitoring and analysis techniques, security teams can help protect their organization's assets, detect security incidents,

	and respond to threats in a timely and effective manner.
Respond	To contain cybersecurity incidents and affected devices, the following procedures can be implemented: Isolate affected devices from the network to prevent the spread of the attack. Shut down affected services or applications to prevent further damage. Implement firewalls and access control lists to block traffic from known malicious sources. Change passwords and revoke access for any affected user accounts. To neutralize cybersecurity incidents, the following procedures can be implemented: **Implement intrusion prevention and detection systems** to identify and block attacks. **Conduct a forensic analysis of affected systems** to identify the root cause of the incident. **Patch vulnerabilities and update security controls** to prevent similar incidents in the future. **Work with law enforcement** to identify and track down the attackers. The following data or information can be used to analyze this incident: **Network logs and traffic data** to identify the source of the attack and the traffic patterns associated with it. **System logs** to identify any unusual activity on affected devices. **Configuration data** to determine any weaknesses in security controls. **Reports from employees** who may have noticed suspicious behavior prior to the incident. To improve the organization's recovery process for future cybersecurity incidents, the following procedures can be implemented: **Develop and test incident response plans** to ensure that all personnel are aware of their roles and responsibilities in the event of an incident. **Implement backup and recovery procedures** to ensure that data can be restored quickly in the event of an incident. **Develop procedures** for communicating with employees, customers, and other stakeholders in the event of an incident.

	Conduct regular security awareness training to ensure that employees are aware of the latest threats and how to respond to them.
Recover	To help the organization recover from the cybersecurity incident, the following steps can be taken: **Identify the affected systems**: The first step in the recovery process is to identify which systems were affected by the attack. This will help to prioritize the recovery efforts. **Isolate affected systems**: Once the affected systems have been identified, they should be isolated from the rest of the network to prevent further damage and contamination. **Assess the damage**: Once the affected systems have been isolated, the damage caused by the attack should be assessed. This will help to determine the extent of the damage and what data has been compromised. **Restore data from backups**: If data has been lost or corrupted, it should be restored from backups. It is important to ensure that the backups are clean and free from any malware. **Apply security updates**: Once the systems have been restored, all security updates and patches should be applied to ensure that they are up-to-date and protected against future attacks. **Educate employees**: It is important to educate employees about the incident and what steps are being taken to prevent future attacks. This will help to prevent similar incidents from happening in the future. To recover immediately, it is important to have up-to-date backups of all critical data, so it can be restored quickly without having to pay any ransom or lose any data. The organization should have a documented incident response plan that outlines the steps to be taken in case of a security incident. This plan should

	be reviewed regularly and updated as necessary. The plan should include details of who is responsible for what actions, contact details for all key personnel, and details of any third-party support services that may be required. The organization should also have a disaster recovery plan in place, which outlines the steps to be taken in the event of a major incident that affects the entire organization. This plan should include details of how critical systems can be restored, how data can be recovered, and how business operations can be resumed.