Incident report analysis

Date: May 22, 2023

Analyst: Elvis Rafael Gross Cardero

Summary	This morning, an intern reported to the IT department that they were unable to access their internal network account. Access logs revealed that their account had been actively accessing the customer database, despite lacking the necessary permissions. The intern mentioned receiving an email instructing them to visit an external website and log in with their internal network credentials to retrieve a message. We believe this was used as a method by a malicious actor to gain access to our network and the customer database. Furthermore, several employees have noticed missing customer records or the presence of incorrect data in the database. It appears that not only were customer data exposed to a malicious actor, but also some records were deleted or manipulated.
Identify	Attack type: Distributed Denial of Service (DDoS) Attack Affected systems: Internal network of the organization During the attack, network services became unresponsive due to the influx of incoming ICMP packets.
Protect	To further protect the organization's assets and prevent future compromises, the following updates or changes to systems and procedures are recommended:

	Firewall configuration: Update and properly configure the network firewall to effectively block and filter unauthorized incoming ICMP packets. This will help prevent similar attacks in the future and ensure stricter control of network traffic. Password security policies: Implement a strong password policy that promotes the use of secure and unique passwords for each user account. Additionally, employees should be educated and made aware of the importance of not sharing passwords and using secure methods for storing them. Network traffic monitoring: Implement a network monitoring solution that allows for the detection and analysis of abnormal traffic patterns. This will help identify suspicious activities, such as incoming ICMP packets from untrusted IP addresses, and enable early response to potential security incidents.
Detect	To detect similar incidents in the future, the following actions are recommended: Implement network traffic monitoring tools: Utilize network traffic monitoring tools that enable continuous monitoring of traffic on network devices. This will help identify suspicious activity and potential attempts to compromise network security. Establish activity logs: Maintain detailed activity logs of network devices and systems. This will allow for in-depth analysis in case of incidents and help identify patterns and trends that may indicate potential threats.
Respond	For future cybersecurity incidents, a response plan should include: Incident containment: Establish clear and practical procedures to contain cybersecurity incidents and the affected devices. This may involve isolating compromised systems, disabling affected services, and implementing countermeasures to halt the incident's propagation. Data and information analysis: Identify relevant data and information that

	can be used to analyze future security incidents. This may include activity logs, firewall records, and network traffic monitoring data. Enhancement of recovery process: Evaluate and improve the organization's recovery process to effectively handle future cybersecurity incidents. This may include updating recovery plans, training personnel, and implementing additional mitigation measures.
Recover	To assist the organization in recovering from the cybersecurity incident, the following steps should be considered: Identification of critical information: Identify the necessary information that needs to be immediately restored, such as data backups, network configurations, and activity logs. Recovery processes: Establish and follow defined recovery procedures to restore the affected devices, systems, and processes. This may involve system reinstatement, data restoration from backups, and integrity verification of data.

Reflections/Notes: In summary, implementing the mentioned recommendations will help strengthen the organization's security and reduce the risk of future cybersecurity incidents. It is essential to adopt a proactive and continuous approach to monitor, protect, detect, and respond to potential threats.

Sincerely,

Elvis Rafael Gross Cardero

Cybersecurity Analyst Jr.