Tanya Gonzalez
Case: Indecent report analysis with NIST-CSF
For: Marketing, Inc.

Incident report analysis

Summary	Earlier today, a staff member from the human resources department informed the IT department about their inability to access their internal network account. Upon reviewing the access logs, it was evident that despite being locked out of the account, there were active instances of accessing records in the customer database. The staff member mentioned receiving an email urging them to visit an external website and log in using their internal network credentials to retrieve a message. It is believed that this method was employed by an unauthorized individual to gain entry into our network and customer database. Additionally, a few other employees have noticed discrepancies in several customer records, including missing or altered information. This indicates that not only was customer data exposed to a malicious actor, but also some data was deliberately deleted or manipulated. To compound matters, the company experienced a security incident where all network services suddenly became unresponsive. The cybersecurity team determined that this disruption resulted from a distributed denial of service (DDoS) attack, specifically through a deluge of incoming ICMP packets. As a response, the team promptly took action by blocking the attack and temporarily halting non-essential network services, allowing for the restoration of critical network services.
Identify	The company experienced an ICMP flood attack, perpetrated by malicious actors, causing a widespread disruption across the entire internal network. In response, immediate measures were taken to secure and reinstate critical network resources, ensuring their functionality. Concurrently, the incident management team launched a thorough assessment of the attack's impact on systems, devices, and access protocols, with the goal of identifying any weaknesses in security measures. Subsequent findings revealed that an employee's login details had been acquired by the malicious attacker, leading to unauthorized entry into our customer database.

	Initial observations indicate deliberate deletion of certain customer data during the breach.
Protect	In an effort to enhance network security, the cybersecurity team implemented measures to mitigate the risk of ICMP-based attacks. By introducing a new firewall rule, the team limited the rate of incoming ICMP packets, while also deploying an IDS/IPS system to identify and filter out suspicious ICMP traffic based on specific characteristics. To prevent future attacks, the team implemented robust authentication policies. These include the adoption of multi-factor authentication (MFA), restricting login attempts to three tries, and conducting comprehensive training for all employees on the importance of safeguarding their login credentials. Additionally, the company plans to enhance its network security infrastructure by implementing a fortified firewall configuration and investing in an intrusion prevention system (IPS).
Detect	Strengthening network security was a key objective for the cybersecurity team, prompting the implementation of various measures. By configuring the firewall, they established source IP address verification, enabling the identification of any falsified IP addresses in incoming ICMP packets. Complementing this, the team integrated network monitoring software, which facilitated the early detection of unusual traffic patterns that might indicate potential security breaches. To enhance their capacity to detect unauthorized access attempts in the future, the team adopted a proactive approach. They introduced a firewall logging tool and an intrusion detection system (IDS), which will enable comprehensive monitoring of all incoming internet traffic. This will equip the team with the necessary tools to swiftly identify and respond to any instances of unauthorized access.
Respond	The cybersecurity team has devised a comprehensive strategy to prepare for future security incidents. In the event of an incident, they will swiftly isolate affected systems to minimize disruptions and focus on restoring critical

	services. Network logs will be diligently analyzed to uncover any suspicious activity. Transparency and accountability are prioritized, with prompt reporting to upper management and legal authorities as required. As a response to the current situation, the employee's network account has been disabled, and comprehensive training sessions have been conducted to emphasize the importance of safeguarding login credentials. Upper management has been promptly informed, and a proactive approach will be taken to notify affected customers about the data breach. All necessary reporting obligations will be fulfilled in compliance with local regulations.
Recover	To recover from a DDoS attack caused by ICMP flooding and restore network services to their normal functioning state, the cybersecurity team will take a series of steps. In future incidents involving external ICMP flood attacks, the firewall will be utilized to block such threats. The next course of action involves temporarily halting all non-critical network services to reduce internal network traffic. Once this is done, the team will prioritize the restoration of critical network services. Following the timeout of the flood of ICMP packets, all non-critical network systems and services can be brought back online, ensuring a comprehensive recovery process. Additionally, to address the deleted data, the team plans to restore the database from the full backup taken the previous night. It has been communicated to the staff that any customer information entered or modified on the day of the attack will not be available in the backup. Therefore, the staff will need to re-enter the information once the database has been successfully restored from the previous night's backup.
Reflection/Notes	The results achieved in addressing the DDoS attack and data deletion incident demonstrate the effectiveness of employing the NIST framework tools. By utilizing the NIST framework, specifically the tools provided, the cybersecurity team successfully navigated the recovery process. The implementation of measures such as blocking external ICMP flood attacks at the firewall,

	temporarily stopping non-critical network services, and prioritizing the restoration of critical services showcases the team's adherence to the NIST framework's guidelines. Furthermore, the team's decision to restore the database from the previous night's backup aligns with the NIST framework's emphasis on data recovery and restoration. Overall, the incident highlights the importance of leveraging the NIST framework tools to effectively respond to and recover from security events, ensuring the resilience and protection of the network infrastructure.