**Incident report analysis**

**Instructions**

| **Summary** | This morning, an intern reported being locked out of her internal network account. However, access logs show her account was actively interacting with the customer database. She also received a phishing email directing her to an external site to input her credentials. This is believed to be the method through which a malicious actor gained access to the network and customer database. Additionally, other employees have observed missing or incorrect customer records, suggesting that data was not only exposed but also deleted or manipulated by the attacker. | | |
| --- | --- | --- | --- |
| Identify | The incident management team conducted an audit of the systems, devices, and access policies involved in the attack to pinpoint security vulnerabilities. The audit revealed that a malicious actor had obtained an intern's login credentials, which were then used to access the customer database. Preliminary findings indicate that some customer data was deleted as a result of this unauthorized access. | | |
| 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 future unauthorized access attempts, the team will deploy a firewall logging tool and an intrusion detection system (IDS) to continuously monitor all incoming internet traffic. This will help identify and respond to suspicious activity in real time. | | |
| Respond | The team has disabled the intern's network account and provided training to all interns and employees on safeguarding login credentials. Upper management has been informed of the breach and will notify customers by mail about the incident. Additionally, management will report the breach to law enforcement and other relevant organizations, as required by local regulations. | | |
| Recover | The team will restore the deleted data by reverting the database to last night’s full backup. Staff have been informed that any customer information added or modified this morning will not be included in the restored data and will need to be manually re-entered once the restoration is complete. | | |

| Reflections/Notes: The company faced a security incident involving a DDoS attack via an ICMP flood, which caused all network services to stop responding. The cybersecurity team quickly blocked the attack and shut down non-critical services to prioritize restoring critical ones. To enhance protection, they implemented a firewall rule to limit ICMP traffic and deployed IDS/IPS systems. Detection measures included configuring IP verification and network monitoring to identify abnormal traffic. For future incidents, the team plans to isolate affected systems, restore critical services, analyze logs for suspicious activity, and report to management and authorities as needed. Recovery efforts focus on gradually restoring all network services and preventing future ICMP flood attacks. |
| --- |