CyberSecurity Incident Response Project (NIST CSF)

Mythreya Hardur Madhukeshwara

10/12/24

Cyber Security Incident Response Project

Project Overview:
In this project , I will create an incident report for a fictional scenario involving fictional people and a fictional company. Any similarities to real life is not by design, but purely coincidence. I will analyze the situation using the National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF).

Scenario

HexaNet Solutions, a cloud services provider, experienced a ransomware attack that compromised its production database hosted on AWS and internal financial systems. The attack originated from a spear-phishing email and resulted in the exfiltration and encryption of customer data.

Incident Overview

- Attack Type: Ransomware Attack
- Attack Vector: Spear-phishing email with a malicious PDF attachment
- Affected Systems: Cloud-hosted production database, internal financial systems

Detailed Attack Timeline

1) **Initial Access**: On October 1, 2024, an employee in the finance department (Alice Williams) receives a spear-phishing email containing a malicious attachment. The attacker

masquerades as a known vendor (SecurePayments Inc.) with a fake PDF invoice that actually contains a Trojan.

2) **Execution**: When Alice opens the attachment, it drops a payload that establishes a foothold on her workstation. The malware remains dormant for 48 hours to avoid detection and then connects to a Command-and-Control (C2) server to download additional tools for lateral movement.

3) **Lateral Movement**: Using Alice's credentials, the attacker gains access to the company's internal financial systems, escalating privileges to an administrator account. The attacker then moves to the cloud environment and accesses the production database hosted in AWS.

4) **Data Exfiltration and Encryption**: The attacker exfiltrates a large volume of customer data (approximately 100,000 records) and deploys ransomware on both the on-premise financial systems and the cloud database, encrypting all data.

5) **Ransom Demand**: On October 10, 2024, HexaNet Solutions' IT staff notices unusual activity, including encrypted files and a ransom note demanding $3 million in cryptocurrency within 72 hours to decrypt the data.

6) **Detection and Response**: The SOC (Security Operations Center) detects the anomaly through SIEM logs. Further investigation reveals the ransomware and exfiltration. HexaNet Solutions immediately disconnects infected systems from the network and notifies key stakeholders. They also engage external cybersecurity consultants to help with the investigation and recovery process.

NIST CSF Analysis

1. Identify

HexaNet conducted a comprehensive risk assessment in 2023, classifying its cloud-based production database and internal financial systems as critical. While these assets were identified as high-value targets, the risk of phishing attacks was not fully mitigated, leading to this incident. Phishing awareness training was inconsistent, and incident response exercises focused on more traditional attacks.

2. Protect

- Access Control: Employee privileges were not restricted enough. The attacker, after compromising Alice Williams' credentials, could escalate privileges and move laterally within the internal network.
- Data Security: Data was encrypted both in transit and at rest. However, after the attacker

exfiltrated the data, it was encrypted by ransomware, which prevented immediate recovery.
- Employee Training: Phishing training was offered but no recent simulation tests were conducted to assess its effectiveness. Lack of awareness of spear-phishing led to the successful compromise.
- Technology: HexaNet had perimeter defense with firewalls and antivirus but lacked a modern Endpoint Detection and Response (EDR) system, leaving endpoints vulnerable to advanced threats.

3. Detect

- SIEM (Security Information and Event Management) systems in place alerted HexaNet’s SOC (Security Operations Center) of unusual file encryption activity. However, the alert came after the attacker had already exfiltrated customer data due to insufficient monitoring of outbound traffic.
- The organization did not have a cloud-native detection system that could analyze user behavior across AWS services. This gap allowed the exfiltration to occur without immediate detection.
- Anomaly detection systems identified unusual traffic from Alice Williams’ workstation 48 hours after the initial compromise, but this delay limited HexaNet’s response time.

4. Respond

- Incident Response Plan: HexaNet’s incident response team followed the predefined plan, isolating infected systems from the network and escalating the issue to external cybersecurity experts.
- Containment: Infected systems were immediately isolated, preventing the ransomware from spreading to other critical infrastructure. Backups were initiated to ensure recovery.
- Communication: Stakeholders were notified within 24 hours, and customer notification was initiated within 72 hours as part of compliance requirements.
- Mitigation: After isolation, a forensics team was hired to conduct a thorough investigation and analyze the breach's scope.

5. Recover

- Systems and data were restored from secure, regularly maintained backups. The recovery time was approximately 72 hours, during which HexaNet's services remained partially unavailable.
- Following the incident, HexaNet implemented key improvements such as deploying an EDR solution and expanding the SIEM to cover AWS environments. Phishing awareness was strengthened through bi-annual simulation exercises.
- A post-incident analysis resulted in updates to the incident response plan, improving the

speed of detection and response for future incidents.

6. Summary

HexaNet Solutions, a cloud services provider, experienced a ransomware attack triggered by a spear-phishing email sent to an internal employee. The attacker gained access to the company's network, exfiltrated sensitive customer data from its cloud infrastructure, and deployed ransomware, encrypting both cloud-hosted and on-premise systems. The incident caused a 72-hour outage, with potential exposure of customer information. HexaNet's incident response team isolated the infected systems, engaged external cybersecurity experts for investigation, and initiated recovery measures. Following the attack, HexaNet conducted a thorough post-incident analysis and improved its security posture by implementing advanced detection tools and enhanced employee training.

From a NIST Cybersecurity Framework perspective: HexaNet's Identify function revealed gaps in addressing phishing threats, despite having a solid risk assessment for critical cloud and financial systems. For Protect, HexaNet had encryption and antivirus tools but lacked stronger access controls and employee training, especially around phishing. During the Detect phase, the company's SIEM detected anomalies after exfiltration had occurred, indicating a need for better cloud-specific monitoring. In Respond, HexaNet followed its incident response plan effectively, isolating affected systems and promptly notifying stakeholders. Finally, in Recover, the company restored operations using backups within 72 hours and improved its security defenses by deploying Endpoint Detection and Response (EDR) and conducting regular phishing simulation exercises to avoid similar incidents in the future.