**Incident report analysis**

**Instructions**

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this chart as a way to practice applying the NIST framework to different situations you encounter.

| **Summary** | Event Description: A ransomware attack targeted our organization, encrypting critical data and demanding payment for decryption keys.  Date of Incident: May 10, 2024  Systems Affected: Financial databases, employee management systems, and internal communication tools.  Initial Detection: Anomaly detected by the intrusion detection system (IDS) followed by multiple user reports of inaccessible files. | | |
| --- | --- | --- | --- |
| Identify | Technology/Asset Management: The attack targeted Windows-based servers hosting financial data and HR systems.  Process/Business Environment: Financial operations and HR processes were severely impacted, causing disruption in payroll and vendor payments.  People: Determine which roles had access to the compromised systems and evaluate if access controls were a factor in the breach. | | |
| Protect | Access Control: Review and tighten access controls; ensure that only necessary personnel have administrative rights.  Awareness/Training: Increase cybersecurity awareness and training for all employees, focusing on recognizing and reporting potential phishing attempts.  Data Security: Implement stronger encryption methods for sensitive data stored on affected systems.  Information Protection Procedures: Update existing policies to include more frequent data backups and off-site storage strategies.  Maintenance: Ensure all systems are regularly updated with the latest security patches.  Protective Technology: Consider upgrading to more advanced firewall and intrusion prevention systems. | | |
| Detect | Anomalies and Events: Utilize a more robust SIEM system to integrate logs and alerts for better anomaly detection.  Security Continuous Monitoring: Increase the frequency and scope of network monitoring to detect irregularities more effectively.  Detection Processes: Implement a more sophisticated IDS that includes heuristics and behavior-based detection technologies. | | |
| Respond | Response Planning: Develop a specific ransomware attack response plan including isolation of affected systems and communication protocols.  Communications: Standardize communication procedures to notify IT staff and affected end-users in the event of security breaches.  Analysis: Conduct post-incident analysis to understand the attack vectors and entry points.  Mitigation: Practice immediate isolation of infected systems to prevent spread and detailed forensic analysis to remove the threat.  Improvements: Review and refine incident response strategies regularly based on lessons learned from incidents. | | |
| Recover | Recovery Planning: Create detailed recovery plans that prioritize system restoration and data recovery without paying the ransom.  Improvements: Integrate learnings from current and past incidents to strengthen recovery strategies and infrastructure resilience.  Communications: Develop clear guidelines on how recovery efforts are communicated internally and externally to minimize confusion and ensure transparency. | | |

| **Reflections/Notes:**  This incident highlights the need for continuous improvement in cybersecurity practices across all functions of the NIST CSF.  Regular training and updated response protocols are crucial in mitigating the impact of such attacks.  The importance of proactive protection and detection strategies was evident, as earlier detection could have potentially minimized damages.  The recovery phase underscored the value of having robust backups and an incident recovery plan tailored to different types of cyber threats. |
| --- |