Incident Response Plan for Target: Point-of-Sale (POS) Malware Attack

---

Incident Type: Malware Attack
The Target breach involved malware installed on POS terminals, which allowed attackers to capture credit card data as it was processed.

1. Detection

- **Method**: Use a **Security Information and Event Management (SIEM)** system with advanced behavioral analysis. This setup monitors traffic patterns, detects abnormal activities (e.g., POS terminals communicating with unknown IP addresses), and alerts the security team to potential malware activity.

2. Containment Strategy

- **Immediate Action**: **Isolate the infected POS systems** from the rest of the network to stop further spread of the malware and secure any unaffected systems.
- **Segmented Access**: Restrict network communication for systems interacting with payment processing networks to reduce the malware's reach across other endpoints.

3. Eradication Steps

- **Remove Malware**: Use endpoint detection and response (EDR) tools to thoroughly scan and remove all instances of the malware from the POS systems and other potentially compromised areas.
- **Patch Vulnerabilities**: Apply patches and security updates to fix vulnerabilities in the POS software or other systems identified during the investigation.

4. Recovery Steps

- **Restore Data**: Reinstall secure, malware-free versions of the POS software and restore any affected systems from secure backups.
- **Implement Enhanced Security Controls**: Set up continuous monitoring and multi-layered authentication for POS systems and network segments handling sensitive data.
- **User and Customer Notification**: Notify affected customers, offering support services such as credit monitoring to those impacted by the data breach.

Type of Attack: Malware

- **Explanation**: Malware is malicious software that can infiltrate systems to steal data, disrupt operations, or gain unauthorized access. In this case, malware was used to intercept and transmit sensitive payment card information to attackers.

Legal and Ethical Compliance in Incident Response Plan

In any incident response plan, adherence to legal and ethical standards is crucial. This section outlines the relevant laws, ethical considerations, and how the incident response plan ensures compliance.

Relevant Laws and Regulations

1. **General Data Protection Regulation (GDPR)**:
    - **Overview**: The GDPR is a comprehensive data protection law in the European Union that establishes guidelines for the collection and processing of personal information of individuals within the EU. It mandates that organizations protect personal data and privacy and imposes strict penalties for non-compliance.
    - **Relevance**: In the event of a data breach, organizations must notify affected individuals and relevant authorities within 72 hours of becoming aware of the breach. The incident response plan includes procedures for prompt notification, ensuring compliance with GDPR requirements.
2. **Health Insurance Portability and Accountability Act (HIPAA)**:
    - **Overview**: HIPAA is a U.S. law that provides data privacy and security provisions for safeguarding medical information. It mandates that healthcare providers and their partners protect sensitive patient data.
    - **Relevance**: In the case of a security incident involving protected health information (PHI), organizations must report breaches to affected individuals and the Department of Health and Human Services (HHS). The incident response plan specifies protocols for reporting and managing breaches of PHI to uphold HIPAA regulations.

Ethical Considerations

- **Transparency**: An ethical consideration in incident response is the commitment to transparency with stakeholders (employees, customers, and regulators) regarding data breaches and the organization's response. Ethical behavior involves being open about the nature of the breach, how it occurred, and the steps being taken to mitigate harm.
- **Data Minimization**: Ethical data handling also includes the principle of data minimization, where organizations should only collect and retain data that is necessary for their operations. This reduces the risk of exposing unnecessary information during a breach.

Upholding Legal and Ethical Compliance

The incident response plan is designed to align with legal requirements and ethical principles in the following ways:

- **Training and Awareness**: Regular training for employees on legal obligations under GDPR and HIPAA ensures they understand the importance of compliance and ethical behavior in handling sensitive data.
- **Incident Reporting Procedures**: Clear procedures are established for reporting incidents in accordance with GDPR and HIPAA, including timelines for notification. The plan ensures that all stakeholders are informed promptly, thus maintaining transparency.
- **Data Protection Measures**: The plan outlines the implementation of technical and organizational measures to protect sensitive data, which aligns with ethical standards of data protection and minimizes the risk of breaches.
- **Post-Incident Review**: Following an incident, the response plan includes a review process to analyze the breach, determine its causes, and implement changes to policies and procedures, ensuring continuous improvement and accountability.

By incorporating these legal and ethical considerations, the incident response plan not only aims to mitigate the impact of security breaches but also fosters trust and integrity in the organization’s operations.