Oksana Syvun

Illustrative Incident Response Plan: Simulated Data Breach Scenario

Documenting incident response proficiency for portfolio showcase

Disclaimer (in case the README file is not read):

This Incident Response Plan (IRP) is a hypothetical document crafted for training, illustrative, and skill-showcasing purposes. The scenario presented, involving a data breach due to a web application vulnerability, is entirely fictional. Any resemblance to real entities or situations is coincidental.

The IRP has been developed with inspiration from recommendations and best practices outlined in the "Computer Security Incident Handling Guide" provided by the National Institute of Standards and Technology (NIST). It serves as a demonstration of the creator's understanding of incident response principles and methodologies.

The intention behind publishing this IRP on GitHub is to showcase the creator's skills to potential employers and the GitHub community. Organizations are encouraged to consult authoritative sources, adapt, and tailor incident response plans to their unique environments.

Users are reminded that this document is not a substitute for professional advice, and its use is at the discretion of the reader. The creators of this document assume no liability for its use, and users are urged to exercise caution and seek professional guidance when developing incident response plans for their specific needs.

The creator appreciates feedback and contributions from the GitHub community to enhance the educational value of this project.

Introduction:

In this hypothetical scenario, the incident involves a data breach where sensitive customer data is compromised due to a vulnerability in a web application. The breach poses a significant risk to the confidentiality and integrity of the affected data. The primary objective of this Incident Response Plan (IRP) is to swiftly and effectively respond to the breach, mitigate the impact, and secure the compromised data. The plan aligns with the recommendations outlined in the "Computer Security Incident Handling Guide" from the National Institute of Standards and Technology (NIST).

General objectives :

- **Demonstrate incident response proficiency:**

  Showcase a comprehensive understanding of incident response principles, methodologies, and best practices in addressing a simulated data breach scenario.

- **Illustrate adherence to NIST guidelines:**

  Align the IRP with the recommendations outlined in the "Computer Security Incident Handling Guide" from the National Institute of Standards and Technology (NIST).

- **Provide a hypothetical framework:**

Offer a structured and hypothetical framework for responding to a data breach resulting from a web application vulnerability.

- **Showcase skill set to employers:**

Demonstrate incident response skills and capabilities to potential employers, emphasizing the ability to develop and implement effective incident response plans.

- **Contribute to community education:**

Contribute to the educational resources available in the cybersecurity domain by publishing the IRP on GitHub, inviting feedback, and fostering knowledge-sharing within the community.

- **Encourage collective knowledge sharing:**

Foster a culture of collective knowledge sharing within the cybersecurity community by actively participating in discussions, sharing insights, and collaborating on improvements to the IRP.

Incident Response Plan: Simulated Data Breach Scenario

1. Preparation:

- Establish a clear objective to minimize the impact of the data breach and protect sensitive customer data.
- Identify and designate roles within the incident response team, including Incident Manager, Technical Analysts, Communication Liaison, and Legal Advisor.
- Conduct regular training sessions to ensure the incident response team is well-prepared and aware of their roles and responsibilities.
- Maintain up-to-date documentation for critical systems, network architecture, and contact information for key personnel.

2. Detection:

- Implement continuous monitoring tools and intrusion detection systems to detect unusual activities or signs of a potential compromise.
- Classify incidents based on severity and impact, with a focus on scenarios involving sensitive customer data.
- Establish communication channels for prompt notification of the incident response team and relevant stakeholders.

3. Containment:

- Isolate affected systems to prevent further unauthorized access to sensitive customer data.
- Apply patches promptly to address the web application vulnerability and prevent further exploitation.

4. Eradication:

- Conduct a thorough investigation to identify the root cause of the vulnerability and take corrective actions to eliminate it.
- Apply necessary updates and configurations to prevent a similar incident in the future.

5. Recovery:

- Restore affected systems from clean backups once the vulnerability is patched.
- Communicate transparently with affected customers, providing information and reassurance.

6. Lessons Learned:

- Conduct a comprehensive review of the incident, identifying strengths and areas for improvement.
- Update incident response documentation based on lessons learned.

7. Communication:

- Keep internal stakeholders informed about the incident response progress.
- Communicate transparently with customers and regulatory bodies as required.

8. Legal and Compliance:

- Engage legal advisors to ensure compliance with data protection laws and regulations.
- Report the incident to relevant authorities if required by law.