STUDENT: INCIDENT RESPONSE

Document Version: 2018-10-03

This material is based upon work supported by the National Science Foundation under DUE #1501990. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Contents

Overview

This project includes the following tasks:

1. Review the incident response documents
2. Analyze the scenario
3. Determine the impact of a significant data breach

Objective: Developing an Incident Response Questionnaire

Incident response is the way an organization addresses and manages a security breach or an attack, i.e., the incident. The goal of the organization is to handle the matter in a way that limits damage and reduces recovery time.

An incident response plan includes a policy that details what constitutes an incident. An **incident response procedure** is a systematic process that the organization follows when an incident occurs.

The Critical Incident Response Team (CIRT) leads the organization's response to the security incident. The members of CIRT include security and general IT staff, and may include employees from legal, human resources, and public relations.

According to SANS, there are six steps to handling incidents:

1. Preparation: A team is ready to handle an incident at a moment's notice. This includes an established policy, a response plan/strategy, a communication plan, a documentation plan, a team, access control, tools, and training.
2. Identification: Includes collection of evidence to determine the scope and documentation of the event.
3. Containment: Limits the damage and prevents further damage, including short-term containment, system back-up, and long-term containment.
4. Eradication: Removes and restores affected systems, always with documentation; usually includes improving defenses to prevent further incidents.
5. Recovery: Carefully returning affected systems back into the production environment, ensuring another incident does not ensue.
6. Lessons learned: Complete documentation of the incident to benefit handling of future incidents, covering the details of who, what, where, why, when, and how questions, usually essential to a "lessons learned meeting."

Staff and administrators who manage IT resources must be aware of the procedures in place to recover from an information security incident. The procedure also enables incident response in a methodical manner in order to carry out all necessary steps to handle an incident correctly. The proper implementation of this procedure minimizes disruption of critical computing services while minimizing the loss or theft of sensitive or mission critical information.

If the data breach affects critical data on the compromised system, the Critical Incident Response (CIR) procedure should be followed.

Supplemental Materials

Website Links

The Incident Handler's Handbook

REN-ISAC.net

PCI ComplianceGuide.org

Project Scenario

The responsibility of an information security professional is to protect the digital assets of XYZ College. You must follow cybersecurity standards and monitor incoming and outgoing traffic in order to detect malicious activity entering or exiting the network.

All IT security personnel must read and sign off on the college's policies. One of these policies is the Incident Response Policy.

The Problem:

The XYZ College Chief Information Office (CISO) just received a potential data breach report from the Research and Education Networking Information Sharing and Analysis Center (REN/ISAC).

The report specifically identifies credentials of XYZ College students that appear in a credential dump on a well-known black hat public website. Below is the notification received from REN-ISAC:

> Greetings. It has been brought to the attention of REN-ISAC that some credentials from your institution have appeared in a credential dump. Most of these credential dumps are discovered on publicly accessible sources. These credentials may be the actual sets used to access your institution's information resources or it may be users utilizing their email at a third-party site. Even if the credentials are not used on your institution's information resources, it may be worth investigating as these credentials are sometimes captured via password stealers. Additionally, users often use their passwords across multiple accounts at different sites.
>
> We have no way of determining when the credentials were stolen/acquired. We only know that they have been disclosed within the last few days. This means we are unable to determine if the accounts listed are current, active, or years old.

Two days before the notification from REN/ISAC, a student reported that he received erroneous charges from the college on his account.

1 Review Incident Response Documents

1. Review the project scenario above. Document the critical facts. Identify the individuals and IT resources impacted by the event presented.
2. Meet with your partner to review the ***Data Breach Policy*** and the ***Procedure for Breach*** handouts.
3. Using the *Incident Response Workflow Process* found in the ***Procedures for Breach*** handout, diagram the incident.

2 Analyze the Scenario

2.1 Review the project scenario and memo

1. Review the ***Memo from XYZ College*** handout sent by the system owner of the affected system.
2. Identify each piece of information shared and use this information to make decisions using the *Incident Response Workflow Process*.

2.2 Create an Incident Response Questionnaire

1. Open the ***Questionnaire*** handout.
2. Use the *Project Scenario*, *Memo*, *Incident Response Policy*, and *Data Breach Procedure* to construct ten questions that will capture relevant data required to determine the type of incident response process required.
3. Review the *CIR Investigation Form* (within the ***Questionnaire*** handout) and determine if this incident will trigger the CIR process (provide specific support for your position).

3 Determine the Impact of a Significant Data Breach on an Organization

1. As a class, be prepared to discuss the impact of a significant data breach on an organization's operations, reputation, legal liability, and financials.
2. Discuss the need for effective incident response in protecting an organization's information technology assets.
3. Describe the steps and components of a good incident response procedure.
4. Complete the *CIR Investigation Form* for this incident.

Conclusion

An incident response procedure provides a framework for how an organization protects its assets should a data breach or security incident occur. This project examines why an organization designates a team to respond to incidents within the organization. This project also explored how an organization determines if the incident should trigger a CIR-level investigation.