Introduction to Incident Response

Reading

40m

Status Incomplete

Introduction

Information security, at its core, is about the safety and protection of an organization's core systems and data from potentially damaging incidents. These incidents could be anything from unauthorized access to sensitive data to malicious code seeking access to internal systems.

Everything an organization does to be ready for one of these situations is part of its contingency plan (CP). Understanding the incident response (IR) is a major part of any CP as a security professional, as it outlines the process to identify, assess, and resolve the challenge.

Reading

Information Security Policies

Information security policies are documents that outline the processes and measures that should be in place for an organization based on the risk or criticality of the system to be vulnerable. These policies can be used to create a set of standards for employees to follow with the aim of assessing and mitigating the risk of the incident, in addition to protecting the organization from liability in the case of any breach or violation of these standards.

Risk management is a process by which organizations identify potential threats to their assets, prioritize them based on their likelihood and impact level, and then implement strategies to mitigate those threats. The goal is to ensure that any risks are mitigated before they result in an actual loss (such as monetary damage or loss of customer trust). To carry this out, a risk assessment is performed which is a process where you look at all the possible ways in which a threat could occur, as well as how serious it would be if it did occur. Once you've identified those threats, you can begin to create IR plans and responses for preventing them and mitigating their impact.

> A risk assessment may sound familiar. You learned how to prepare a risk assessment report in an earlier course.

During this course you will start building the corresponding incident plans and strategies based on your risk assessment report.

Planning for Organization Readiness

Organizational readiness is essential to corporate security. Contingency planning is the process that ensures an organization is ready for any incidents that may arise. CPs are developed by corporate headquarters and business divisions using the following steps:

- Policy formation
- Analysis and assessment
- Plan development
- Implementation
- Monitoring and evaluation

CPs should enable each unit to create its own strategy depending on its requirements while offering overarching guidelines on how to react to a crisis. The regulations that govern this process should specify who makes emergency choices, what resources are available, and what occurrences need attention.

Contingency Planning

When it comes to ensuring the continuity of your organization's operations, you need a CP. It's that simple.

In the event of an incident or disaster, your organization will have to make sure that critical data and organizational functions are preserved and recovered quickly if they are ever lost. You must also be able to resume critical business processes at alternate sites, in the event your main site is damaged or lost. This is why CPs are so vital.

There are several ways to archive and recover critical information assets, including cloud computing. Cloud computing has altered the organization's approach to both availability and recovery of critical information assets by allowing organizations to use multiple providers as a single system of record, as well as providing a more secure environment for data storage and management.

IR

Everything an organization does to be ready for an emergency is part of its CP. IR is a major part of any CP, and is concerned with the identification and assessment of the severity of new and emergent unexpected occurrences. When an event occurs, the IR process should strive to contain and resolve the issue in accordance with the IR plan. After an incident has been evaluated and determined to be uncontainable or unresolvable, the escalation steps outlined in the CP are implemented.

There are four key stages that make up the IR process:

- Preparation
- Detection and analysis
- Containment, eradication, and recovery
- Post-incident activities

> Since the IR procedure is lengthy and involved, you will simply cover the first steps in this section. The remainder of the IR process, including detection, reaction, and recovery, will be covered subsequently.

Key Takeaways

- Whether the incident is a natural occurrence, or an intentional act, information security policies ensure there is a clear process for employees to follow in the event of an incident to mitigate any risk.
- IR plans are designed to identify, assess, and contain any risk.
- CPs are essential. In the event of a worst case scenario, critical business infrastructure can be recovered and operations can continue.

Conclusion

Incidents are inevitable, and as information security professionals, it is essential that you put the policies and processes in place to be prepared. In the next reading, you'll continue exploring this topic by learning about the IR planning process.

✓ Mark Completed

Previous
Overview - Incident Response

Next
Pre-Incident Planning

How well did this activity help you to understand the content?

Let us know how we're doing

W05D5

Fri Jul 26

W05D5 Schedule »