Incident Handling

Incident Handling Definition & Scope

Incident handling (IH) has become an important part of an organization's defensive capability against cybercrime. While protective measures are constantly being implemented to prevent or lower the amount of security incidents, an incident handling capability is undeniably a necessity for any organization that cannot afford a compromise of its data confidentiality, integrity, or availability. Some organizations choose to implement this capability in-house, while others rely on third-party providers to support them, continuously or when needed. Before we dive into the world of security incidents, let's define some terms and establish a common understanding of them.

An `event` is an action occurring in a system or network. Examples of events are:

- A user sending an email
- A mouse click
- A firewall allowing a connection request

An `incident` is an event with a negative consequence. One example of an incident is a system crash. Another example is unauthorized access to sensitive data. Incidents can also occur due to natural disasters, power failures, etc.

There is no single definition for what an IT security incident is, and therefore it varies between organizations. We define an IT security incident as an event with a clear intent to cause harm that is performed against a computer system. Examples of incidents are:

- Data theft
- Funds theft
- Unauthorized access to data
- Installation and usage of malware and remote access tools

`Incident handling is a clearly defined set of procedures to manage and respond to security incidents in a computer or network environment.`

It is important to note that incident handling is not limited to intrusion incidents alone.

Other types of incidents, such as those caused by malicious insiders, availability issues, and loss of intellectual property, also fall within the scope of incident handling. A comprehensive incident handling plan should address various types of incidents and provide appropriate measures to identify, contain, eradicate, and recover from them to restore normal business operations as quickly and efficiently as possible.

Bear in mind that it may not be immediately clear that an event is an incident, until an initial investigation is performed. With that being said, there are some suspicious events that should be treated as incidents unless proven otherwise.

Incident Handling's Value & Generic Notes

IT security incidents frequently involve the compromise of personal and business data, and it is therefore crucial to respond quickly and effectively. In some incidents, the impact may be limited to a few devices, while in others a large part of the environment can be compromised. A great benefit of having an incident handling team (often referred to as an incident response team) handle events is that a trained workforce will respond systematically, and therefore appropriate actions will be taken. In fact, the objective of such teams is to minimize the theft of information or the disruption of services that the incident is causing. This is achieved by performing investigations and remediation steps, which we will discuss more in depth shortly. Overall, the decisions that are taken before, during, and after an incident will affect its impact.

Because different incidents will have different impacts on the organization, we need to understand the importance of prioritization. Incidents with greater severity will require immediate attention and resources to be allocated for them, while others rated lower may also require an initial investigation to understand whether it is in fact an IT security incident that we are dealing with.

The incident handling team is led by an incident manager. This role is often assigned to a SOC manager,

CISO/CIO, or third-party (trusted) vendor, and this person usually has the ability to direct other business units as well. The incident manager must be able to obtain information or have the mandate to require any employee in the organization to perform an activity in a timely manner, if necessary. The incident manager is the single point of communication who tracks the activities taken during the investigation and their status of completion.

One of the most widely used resources on incident handling is NIST's Computer Security Incident Handling Guide. The document aims to assist organizations in mitigating the risks from computer security incidents by providing practical guidelines on responding to incidents effectively and efficiently.

Next ➜

Mark Complete & Next