Incident response plans

So you've learned about incident response teams, the different types of roles, and
their respective responsibilities.
Now, let's talk about how teams respond to incidents using incident response plans.

When an incident occurs, incident response teams must be prepared to respond quickly, efficiently, and effectively.
Whether it's a data breach, DDoS attack, or ransomware, incidents have the potential to cause significant damage to an organization.
Like we previously mentioned, regulations may require organizations to report incidents within a certain timeframe.
So it's crucial for organizations to have a formal incident response plan in place, so there's a prepared and
consistent process to quickly respond to incidents once they occur.

You may remember learning that security plans consist of three basic elements: policies, standards, and procedures.
An incident response plan is a document that outlines the procedures to take in each step of incident response.

Response plans, just like response teams, are not all the same.
Organizations tailor their plans to meet their unique requirements such as their mission, size, culture, industry, and structure.
For example, smaller organizations may choose to include their incident response plan in their security plan, while others may choose to have them as separate documents.

Although not all incident plans are the same,
there are common elements that they share.

Incident plans have: Incident response procedures.
These are step-by-step instructions on how to respond to incidents.
System information. These are things like network diagrams, data flow diagrams, logging, and asset inventory information.
And other documents like contact lists, forms, and templates.

Plans aren't perfect, and there's always room to adjust and improve as incidents occur.
Incident processes and procedures must be regularly reviewed and tested.

This can be done through exercises like tabletops or simulations.
These exercises ensure that all team members are familiar with the response plan.
They also allow organizations to identify any missing gaps in a process to improve their incident response plan.
Also, organizations may be required to complete specific types of exercises for regulatory reasons.

Coming up, we'll discuss the different types of tools used in incident response.

Revision #1
Created 2023-09-06 10:48:15 UTC by naruzkurai
Updated 2023-11-01 01:10:46 UTC by naruzkurai