tracesecurity

Whitepaper

Incident Response Plan:

What Every Organization Needs

Mitchell Bearry
Information Security Analyst

Introduction

One of the most critical aspects of any business is the ability to sustain a disaster and recover from it. In the present day, this is seen more clearly than ever through the prevalence of cybersecurity incidents that target companies through ransomware, botnets, and data breaches. As this threat increases, the scope of these targets is expanding as well. It is not just financial institutions that are targeted, but also industrial engineering, software, electrical, chemical, and other companies. It is equally as important for each of these types of businesses to have a plan in place for dealing with these attacks when they happen. If an organization is caught unaware and without a plan, it can mean the downfall of the entire company. An Incident Response Plan provides a documented structure for dealing with these threats to ensure that when the time comes, businesses are aware of exactly how to handle the adverse situation and move past it in a timely and efficient manner.

The Steps

While the names of these steps change from organization to organization, in my years of auditing incident response plans, I see a common structure in place at each institution. The steps and their objectives are usually along the lines of what is shown below:

- Preparation: This phase involves all of the planning that occurs prior to an incident occurring.
- Detection: This phase involves the initial identification of an incident, the classification according to severity, and the launch of an investigation to determine the impact.
- Containment: This phase involves isolating, locking down, or otherwise ensuring that the virus or attack on the affected devices does not spread throughout the rest of the devices on the network.
- Eradication: This phase involves purging all systems of the virus or attackers' presence.
- Recovery: This phase involves the recovery back to normal business operations.
- Follow-up: This phase involves documenting lessons learned from the attack and how the organization can improve its processes in the future.

Preparation

It may sound obvious, but the first step in preparing for an incident involves documenting an Incident Response Plan. If an organization wants to ensure that, following discovery of an incident, they are prepared and knowledgeable on how to respond, the best way to do that is to have a predefined plan listing the roles of involved personnel and the guidelines for response. The plan should outline the members of the Incident Response Team, the responsibilities of each member, and the order of operations for response and recovery.

This preparation also includes all of the security controls that are in place across the enterprise to protect, detect, and respond to cyber incidents. This includes approval from the Board of Directors or other governing body for the organization. The most important security control that can be put in place to protect against cyber incidents in particular is backups. Backups of not just the data, but also the full system image should be taken often and stored both locally on separate media as well as offsite or in the cloud. These will prove invaluable in the event of a ransomware or other malware outbreak.

Finally, the best way to ensure an organization is prepared is to do regular testing. Run phishing campaigns to determine the susceptibility of your employees to phishing emails. Perform regular vulnerability scanning and penetration testing to determine the effectiveness of your security software and solutions at detecting and blocking cyberattacks. Most importantly, the plan itself should be tested using tabletop exercises, backup failover tests, and other scenarios to ensure that the plan works and effectively allows the response team to handle incidents. It also ensures that each member of the response team is aware of their roles and responsibilities and can adequately perform their duties.

Detection

Also known as Identification, this step involves the initial detection of a cyber incident and the beginning steps of the response process. Information security incidents can be detected in a number of different ways. The two main instances in which they are identified is either through an employee reporting the event, or a security solution such as an IDS/IPS, endpoint protection solution, or SIEM solution generating an alert. It is also important to note that incidents are not just related to cybersecurity; they can also be physical in nature. With a suspected physical intrusion event, it is likely that an employee will report it. The company monitoring the facility's security alarm may also be the source of the report of an intrusion.

Once an incident has been detected, the first thing that should be done is documentation of the report. This is where incident response tracking forms come in. Each organization should have a template in place that allows them to write down the details of the incident throughout the cycle from initial Detection through Follow-up. When an event is first identified, the first line of response personnel should be documenting how the incident was detected, which system or employee reported it, the time of the detection, and all other associated details of the incident. As the incident response process continues, it is important to continue to record each aspect of the response so it can be used during the investigation process that may follow.

The next part of the process that should also be incorporated into the tracking form is incident classification. Resource management is an important aspect of any business's success, and as a result it is important to avoid contacting and involving personnel in the response process unless necessary. For this purpose, incidents should be categorized by type, severity level, or both in order to determine how critical it is, and which personnel need to be involved. This will also aid in prioritizing incidents as severity levels can determine which ones are most critical to address, as well as provide standards for a timetable on how soon a response needs to occur. The notification requirements should be documented along with contact information for needed personnel.

Containment

Following confirmation that an incident has occurred, the next step is to contain it to prevent the intruders or malware from gaining further or access to the network. It is important to note that the response to an event for both Containment and the following Eradication step should be tailored to the specific severity level or category of incident to ensure the most appropriate response is taken.

While the knee-jerk reaction to ransomware or malware of any other kind is to shut down the machine to keep it from spreading, this is actually the opposite of what should be done. Performing this action could potentially ruin the forensic investigation process and prevent an organization from determining the source of the attack, how many other devices were infected, and destroy evidence of the attack.

Instead, the machine should first be isolated from the rest of the production network. All Internet access should be cut off, and the device should be logically segmented from all other devices to prevent the malware from spreading. This includes any shared storage devices locally to guarantee that the infection cannot propagate further.

This phase is also where the forensic investigation process begins. Once contained, the computer should be scanned using antimalware tools to determine the cause of the infection. A memory dump should be taken of the RAM, as well as local event and audit logs that will show items such as the active users and running services. Once an image of this and all other infected machines has been taken, and all possible data needed to identify and trace the attackers' methods and path, it is safe to proceed to the next step.

Eradication

Also known as Mitigation or Remediation, the Eradication step revolves around a single focus: destroy the malware on the infected devices. Simply stopping the malware services from running or purging it with an antivirus is often not enough as Registry files or other items may have been permanent altered. The best way to make certain that the malware is gone is to completely wipe the drives. In some cases, it may even be necessary to remove the drives and install new ones entirely. If this is done, the drives should be securely destroyed either internally with logs of the destruction, or through a third-party with a certificate of destruction received to verify the process is complete.

If wiping, do not rely on the simple Windows reformatting. The operating system and every other byte of data on the drive should be destroyed. Darik's Boot and Nuke (DBAN) is an example of a simple tool that can be used to do this in accordance with standard 5220.22-M from the Department of Defense. However, while free, this tool may not be as robust or provide the certification of destruction required by more mature organizations. A proper tool for wiping drives securely should be identified and purchased during the Preparation phase to prevent a last-minute acquisition following an emergency.

Recovery

The next step is Recovery. Once the malware has been removed completely from all infected devices, it is time to bring the systems back to full operational status. Some organizations may not want to do this and opt instead to use the opportunity to upgrade systems that were older. If the hard drives were removed entirely and destroyed, new ones should be purchased and installed.

From this point, Windows or other operating systems can be freshly installed, and the data restored using the backups. If the institution can verify that the malware did not affect the local backups, this process should be fairly quick and restore business functions soon. However, if there is a danger of the local backups having been infected, this process may take more time if backups must first be retrieved from an offsite location or downloaded from the cloud.

This is also the step in which the decision on whether to activate the Business Continuity Plan and/or Disaster Recovery Plan should be made. If the incident compounds into a full disaster that requires enterprise-wide or more complicated recovery processes such as relocation of personnel, management should determine if the larger recovery and restoration procedures need to be initiated.

Follow-Up

Also called Post-Incident Review, this step consists of a post-incident meeting and other analysis to assess the performance of the response team, the success of the response, and other factors to

determine if the process performed adequately or if improvements need to be made to the plan and processes.

During these meetings, the incident response form listing the actions taken throughout the incident is reviewed for accuracy. The response and recovery times should be compared with the predefined RTO and RPO metrics to ensure that they were met, or if not to identify whether the metrics themselves need to be adjusted to be more realistic of an actual attack. In addition to analyzing the response, the main goal of this review is to implement the necessary security controls to plug the hole by which the attackers got in and prevent a similar incident from occurring again in the future. Management should be involved in these meetings, and the discussions documented for future reference.

Conclusion

While the names of the incident response phases or exact specifics may vary by organization, this outline of the process should always be included as each of these steps are critical to ensuring that the institution is able to successfully respond to incidents. With proper Preparation and Detection implementation, businesses will often be able to avoid the rest of the steps entirely by mitigating the attack before it is successful.

This entire process should be defined within policies and procedures and regularly consulted for veracity when major changes occur. TraceSecurity provides a number of services by which the Incident Response Plan and other security controls may be assessed for sufficiency, including but not limited to assistance with policy development, audits, tabletop testing, and penetration tests. Please contact us for more information on how to jumpstart or expand your incident response program today!