USAID
FROM THE AMERICAN PEOPLE

DEVELOPMENT OF AN ORGANIZATIONAL INCIDENT RESPONSE PLAN

Enabling Organizations in responding to threats

This publication was produced at the request of the the United States Agency for International Development. It was prepared independently by implementing partner, Catalisto LLC for the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity. The authors' views expressed in this publication do not necessarily reflect the views of the United States Agency for International Development or the United States government.

MODULE 1 - INTRODUCTION

Awareness is growing that all companies, including both enterprises and small- to mid-size organizations, need a cybersecurity incident response plan. No organization, regardless of size, is exempt from cybersecurity threats, and having an established plan of action that immediately executes following a security breach is crucial to limit incident costs and damages to the company's reputation.

Of course, there are hundreds of possible considerations – not to mention moving parts – that must all fit together seamlessly and execute flawlessly for successful incident response. Some companies, particularly those that haven't yet experienced a major security incident, don't know where to begin, let alone what to prioritize.

An incident is a matter of when, not if, a compromise or violation of an organization's security will happen. The preparation of the Computer Incident Response Team (CIRT) through planning, communication, and practice of the incident response process will provide the necessary experience needed should an incident occur within your organization.

Each phase from preparation to lessons learned is extremely beneficial to follow in sequence, as each one builds upon the other. The following phases will provide a basic foundation to be able to perform incident response and allow one to create their own incident response plan.

ABSTRACT

Computer security incident response has become an important component of information technology (IT) programs. Because performing incident response effectively is a complex undertaking, establishing a successful incident response capability requires substantial planning and resources.

This module assists mentees in establishing computer security incident response capabilities and handling incidents efficiently and effectively. The module provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident. The guidelines can be followed independently of particular hardware platforms, operating systems, protocols, or applications.

PREPARATION

This phase as its name implies deals with the preparing a team to be ready to handle an incident at a moment's notice. An incident can range from anything such as a power outage or hardware failure to the most extreme incidents such as a violation of organizational policy by disgruntled employees or being hacked by state sponsored hackers (Bejtlich, 2005).

Regardless of the cause of the incident preparation is the most crucial phase compared to all of the others, as it will determine how well your team will be able to respond in the event of a crises. There are several key elements to have implemented in this phase in order to help mitigate any potential problems that may hinder one's ability to handle an incident. For the sake of brevity, the following should be performed:

1. Policy – a policy provides a written set of principles, rules, or practices within an organization; it is one of the keystone elements that provide guidance as to whether an incident has occurred in an organization. A login banner can be one way to ensure that individuals attempting to log into an organization's network will be aware of what is expected when utilizing an organization's information assets; for example the login banner (dependent upon the local jurisdiction on privacy) can state that all activities will be monitored and any unauthorized users may civil or criminal penalties, etc. Without clear policies, one could leave their organization legally vulnerable to lawsuits, such as an employee being fired for looking at illicit material at work when there was no policy against such behavior within the organization and provided the opportunity for the said individual to be able to file an improper termination lawsuit (Newman, 2007).

2. Response Plan/Strategy – after establishing organizational policies, now it is time to create a plan/strategy to handle incidents. Prioritization of incidents should be based upon organizational impact (Incident Response Process, 2008), for example a single workstation being non-functional can be considered minor, whereas a server being down could be considered a moderate impact (assuming there are backup servers for failover), and data being stolen directly from human resources that contain privileged information as high. The prioritization of the types of incidents based upon organizational impact can help build the case to receive management buy-in, because without management support then it is likely that the CIRT may not be given the resources necessary to properly handle a crisis.

3. Communication – having a communication plan is necessary, due to the fact that it may be necessary to contact specific individuals during an incident. The entire CIRT should know whom to contact, when it is appropriate to contact them, and why. For example, at 12:31pm the online ordering system for a popular e-commerce site during the holiday shopping season went down and no one is able to access the site; it would be prudent to contact the various individuals with specific expertise to get the system back up and running, as well as management to keep them updated as the situation progresses to resolution. By not having a communications plan, then it is likely that response time will be delayed and/or the wrong people would be contacted and one would not have the proper resources necessary to mitigate the problem (Creating a computer security incident response team: a process for getting started, 2006). Please note: it is also necessary to define when it is or is not appropriate to include law enforcement during an incident, due to the consequences that could either positively or negatively affect your organization.

4. Documentation – it is extremely beneficial to stress that this element is particularly necessary and can be a substantial life saver when it comes to incident response. The most significant reason to document an incident is that if the incident is considered a criminal act, then it could be used as

evidence to bring the suspect(s) to justice. The other reason for documentation that is just as important is for lessons learned. It is vital that everything that is done by the CIRT team is documented, that means every action taken (e.g. commands typed, systems affected, etc). Documentation should be able to answer the Who, What, When, Where, Why, and How questions should they ever arise; without such information one could leave a sense of uncertainty if something was called into question, like formatting a hard drive and reinstalling the operating system on a production server (Newman, 2007).

Tip: Checklists with a place for notes, dates and times, and other pertinent information can be extremely handy, especially those that follow each step of incident response.

5. Team – the CIRT should be made up of several people that consist of different disciplines to handle the various problems that could arise during or from an incident. Some of these team members can be attorneys, human resources, public relations, various IT staff with specific specializations, etc. It is particularly beneficial to have an open mind about who is to be included in the CIRT, because some individuals and/or professions may not be as obvious as the actual technical staff to handle an incident (Responding to it security incidents, 2011).

6. Access Control – another key element is to ensure that the CIRT can have the appropriate permissions necessary to perform their job. An excellent example is to have a network or systems administrator being able to add/remove permissions to the accounts of the CIRT during an incident to allow them to mitigate the problem and then have those permissions removed when they are no longer needed (Responding to IT security incidents, 2011).

7. Tools – a CIRT without tools is like kayaking without a paddle, it is inherently difficult to get anything done. It is highly recommended having any available software and hardware that can be readily utilized during an incident; this can range from anti-malware to laptops with packets sniffers, screw drivers and other tools, as well as incident response checklists and other items that would be useful (Bejtlich, 2005). All of the tools one would need during an incident should be contained within a "jump bag" that can be quickly grabbed by CIRT members during an incident.

8. Training – this is a must, because without it your team could be ill prepared and result in a complete failure of handling an incident properly despite the best of planning. It is recommended to have drills at regular interval to insure that each individual within the CIRT is able or knows how to perform their duties during an incident.

CIRT GO-BAG RECOMMENDATIONS

- Incident Handlers Journal to be used for documenting the who, what, where, why, and how during an incident.

- Contact list of all CIRT members.

- Clean USB Drives.

- A bootable USB drive or Live CD with up-to-date anti-malware and other software tools that can read and/or write to file systems of the computing environment that the incident response is to be performed in. One example is that of the Bart's PE disk for Windows XP (or later) environments.

- A laptop with forensic software (e.g. Autopsy, FTK or EnCase), anti-malware utilities, and internet access (if necessary for researching solutions or downloading tools).

- Computer and network tool kits to add/remove components, wire network cables, etc.

- Hard duplicators with write-block capabilities to create forensically sound copies of hard drive images.

- A bag that properly store all of the aforementioned tools in an organized and protective fashion.

IDENTIFICATION

This phase deals with the detection and determination of whether a deviation from normal operations within an organization is an incident, and its scope assuming that the deviation is indeed an incident.

This particular step requires one to gather events from various sources such as log files, error messages, and other resources, such intrusion detection systems and firewalls, that may produce evidence as to determine whether an event is an incident.

If a particular event is determine to be an incident, and then it should be reported as soon as possible in order to allow the CIRT enough time to collect evidence and prepare for the preceding steps (Bejtlich, 2005). At this stage of an incident CIRT members should be notified and communication should be coordinated between members along with designated command center staff (e.g. management and/or systems administrators).

It is recommended that at least two incident handlers be available to handle an incident so that one can be the primary handler who can identify and assess the incident and the other to help gather evidence.

Communication and coordination between members of the CIRT (and management) is critical, especially if the scope of the incident can have a significant impact on business operations.

This is also the phase where incident responders should be documenting everything that they are doing, as stated earlier these documents should be able to answer the Who, What, Where, Why, and How questions in case the documentation is to be used to prosecute the perpetrator(s) in court (Newman, 2007).

After determining the scope of the event and documenting the evidence, then the CIRT team can move forward with the next phase (Incident Response Process, 2008).

A good example of the identification phase is a user contacting the help desk and reporting that their system is acting strangely or intrusion detection systems report unusual network traffic from certain hosts.

It could come from something ominous as usual activity in system logs that have never appeared before a specific date. It is extremely beneficial to keep a truly open mind the number of possibilities that an incident could be identified.

Two other examples worth mentioning are a missing USB drive or other storage media, and a user finding a USB drive somewhere that has public access and plugs into their computer kicking off an auto-run script that steals data or infects systems.

CONTAINMENT

The primary purpose of this phase is to limit the damage and prevent any further damage from happening ("UF IT security," 2011). There are several steps to this phase; however, each one is necessary in order to completely mitigate the incident and prevent the destruction of any evidence that may be needed later for prosecution.

The first step is Short-term Containment; basically, the focus of this step is to limit the damage as soon as possible.

Short-term containment can be as straightforward as isolating a network segment of infected workstations to taking down production servers that were hacked and having all traffic routed to failover servers. Short-term containment is not intended to be a long term solution to the problem; it is only intended to limit the incident before it gets worse (Bejtlich, 2005).

The second step is System Back-Up; it is necessary before wiping and reimaging any system to take a forensic image of the affected system(s) with tools that are well known in the computer forensics community such as Forensic Tool Kit (FTK), EnCase, et al. The reason behind this is that the forensic software will capture the affected system(s) as they were during the incident and thereby preserving evidence in the event that the incident resulted from a criminal act or to be used for observing how the system(s) were compromised during the lessons learned phase (Newman, 2007).

The last step before the next phase is Long-term containment, which is essentially the step where the affected systems can be temporarily fix in order to allow them to continue to be used in production, if necessary, while rebuilding clean systems in the next phase. Basically the primary focus would remove accounts and/or backdoors left by attackers on affected systems, installing security patches on both affected and neighboring systems, and doing other work to limit any further escalation of the incident while allowing normal business operations to continue (Bejtlich, 2005).

A good example of containment is disconnecting affected systems by either disconnect the affected system's network cable or powering down switches and/or routers to entire portions of the network to isolate compromised systems from those that have not been compromised. This in turn will isolate the problem from the rest of the production network and limit the spread of any malware or reduce the risk of further systems being compromised.

ERADICATION

This phase deals with the actual removal and restoration of affected systems. As with each of the prior phases of incident response, continued documentation of all actions taken will be necessary to determine the cost of man hours and other resources as a means of determining the overall impact to the organization. It is also necessary to ensure that proper steps were taken to remove malicious and other illicit content off of the affected systems, and ensuring that they are thoroughly clean (Incident Response Process, 2008). In general that would mean a complete reimaging of a system's hard drive(s) to ensure that any malicious content was removed and prevent reinfection. This phase is also the point where defenses should be improved after learning what caused the incident and ensure that the system cannot be compromised again (e.g. installing patches to fix vulnerabilities that were exploited by the attacker, etc).

A good example of actions performed during the eradication phase would be using the original disk images that were created prior to a system being deployed into production to restore the system and then installing patches and disabling unused services to harden the system against further attacks (e.g. disk images created using software). One would also scan affected systems and/or files with anti-malware software to ensure any malware that is latent is removed (i.e. using an anti-malware software to disinfect systems and scan the Windows registry for keys that may initiate any latent malware).

RECOVERY

The purpose of this phase is to bring affected systems back into the production environment carefully, as to insure that it will not lead another incident. It is essential to test, monitor, and validate the systems that are being put back into production to verify that they are not being reinfected by malware or compromised by some other means. Some of the important decisions to make during this phase are:

- Time and date to restore operations – it is vital to have the system operators/owners make the final decision based upon the advice of the CIRT.
- How to test and verify that the compromised systems are clean and fully functional.
- The duration of monitoring to observe for abnormal behaviors.
- The tools to test, monitor, and validate system behavior.

There are many more beneficial decisions that could be listed; however, the above information should provide a few ideas as what is entailed. The primary goal overall, as stated earlier, is to prevent another incident from happening that was due to the same problems that cause the one that was just resolved (Responding To IT Security Incidents, 2011).

LESSONS LEARNED

The most critical phase after all of the others is Lessons Learned. The purpose of this phase is to complete any documentation that was not done during the incident, as well as any additional documentation that may be beneficial in future incidents. The document should also be written in a form of a report to provide a play-by-play review of the entire incident; this report should be able to answer the: Who, What, Where, Why, and How questions that may come up during the lessons learned meeting. The overall goal is to learn from the incidents that occurred within an organization to improve the team's performance and provide reference materials in the event of a similar incident.

The documentation can also be used as training materials for new team members or as a benchmark to be used in comparison in future crises (Bejtlich, 2005). The lessons learned meeting should be performed as soon as possible; a good rule of thumb is within 2 weeks after the incident. The meeting should go through the incident response report with finalization in an executive summary format. It should be kept short, as to not lose the audience's attention and remain professional.

A good example of performing lessons learned is to have a power point that summarizes the following information:

- When was the problem was first detected and by whom.

- The scope of the incident.
- How it was contained and eradicated,
- Work performed during recovery.
- Areas where the CIRT teams were effective.
- Areas that need improvement.

It should also include time for suggestions and discussion between members of how to improve the overall team. This phase is extremely beneficial to have members share ideas and information in order to improve team effectiveness in future incidents.

INCIDENT HANDLERS CHECKLIST

PREPARATION

1. Are all members aware of the security policies of the organization?
2. Do all members of the Computer Incident Response Team know whom to contact?
3. Do all incident responders have access to journals and access to incident response toolkits to perform the actual incident response process?
4. Have all members participated in incident response drills to practice the incident response process and to improve overall proficiency on a regularly established basis?

IDENTIFICATION

1. Where did the incident occur?
2. Who reported or discovered the incident?
3. How was it discovered?
4. Are there any other areas that have been compromised by the incident? If so, what are they and when were they discovered?
5. What is the scope of the impact?
6. What is the business impact?
7. Have the source(s) of the incident been located? If so, where, when, and what are they?

CONTAINMENT

1. Short-term containment
    a. Can the problem be isolated?
        i. If so, then proceed to isolate the affected systems.
        ii. If not, then work with system owners and/or managers to determine further action necessary to contain the problem.
    b. Are all affected systems isolated from non-affected systems?
        i. If so, then continue to the next step.
        ii. If not, then continue to isolate affected systems until short-term containment has been accomplished to prevent the incident from escalating any further.
    c. System-backup

i. Have forensic copies of affected systems been created for further analysis?

ii. Have all commands and other documentation since the incident has occurred been kept up to date so far?

- If not, document all actions taken as soon as possible to ensure all evidence are retained for either prosecution and/or lessons learned.

- Are the forensic copies stored in a secure location?

    - If so, then continue onto the next step.

    - If not, then place the forensic images into a secure location to prevent accidental damage and/or tampering.

2. Long-term containment

    a. If the system can be taken offline, then proceed to the Eradication phase.

    b. If the system must remain in production proceed with long-term containment by removing all malware and other artifacts from affected systems, and harden the affected systems from further attacks until an ideal circumstance will allow the affected systems to be reimaged.

ERADICATION

1. If possible can the system be reimaged and then hardened with patches and/or other countermeasures to prevent or reduce the risk of attacks?

    a. If not, then please state why?

2. Have all malware and other artifacts left behind by the attackers been removed and the affected systems hardened against further attacks?

    a. If not, then please state why?

RECOVERY

1. Has the affected system(s) been patched and hardened against the recent attack, as well as possible future ones?

2. What day and time would be feasible to restore the affected systems back into production?

3. What tools are you going to use to test, monitor, and verify that the systems being restored to productions are not compromised by the same methods that cause the original incident?

4. How long are you planning to monitor the restored systems and what are you going to look for?

5. Are there any prior benchmarks that can be used as a baseline to compare monitoring results of the restored systems against those of the baseline?

LESSONS LEARNED

1. Has all necessary documentation from the incident been written?
    a. If so, then generate the incident response report for the lessons learned meeting.
    b. If not, then have documentation written as soon as possible before anything is forgotten and left out of the report.
2. Assuming the incident response report has been completed, does it document and answer the following questions of each phase of the incident response process: (Who? What? Where? Why? And How?)?
3. Can a lessons learned meeting be scheduled within two weeks after the incident has been resolved?
    a. If not, then please explain why and when is the next convenient time to hold it?
4. Lessons Learned Meeting
    a. Review the incident response process of the incident that had occurred with all CIRT members.
    b. Did the meeting discuss any mistake or areas where the response process could have been handled better?
        i. If no such conversations occurred, then please explain why?