



INCIDENT RESPONSE PROCESS

JAMES NOLEN

CYBERSECURITY STUDENT AT GREENVILLE TECHNICAL COLLEGE

NOLENJGN@MY.GVLTEC.EDU

“

GIVE ME SIX HOURS TO CHOP DOWN A TREE
AND I WILL SPEND THE FIRST FOUR HOURS
SHARPENING THE AXE.

”

– ABRAHAM LINCOLN, THE 16TH U.S. PRESIDENT

During an incident response, it is important to have a good response plan to protect the organization's data, reputation, and the bottom line.



6 PHASES OF THE INCIDENT RESPONSE PROCESS

1. PREPARATION

2. IDENTIFICATION

3. CONTAINMENT

4. ERADICATION

5. RECOVERY

6. LESSONS LEARNED



PHASE 1 PREPARATION

POLICY, PROCEDURES, AND PRACTICES

Create written documentation of the principles, rules, and best practices. This is often called SOPs (standard operating procedures) or TTPs (tactics, techniques, and procedures). This includes command and control, response planning and strategies, and reporting. The incident responders must understand and follow these to be successful in their incident handling.

EDUCATION AND TRAINING

Obtain knowledge and practice incident response based on established PPPs, SOPs, and TTPs prior to any live event. Learn from previous incidents within and from others outside of the organization. Practice working as a team and handling worst case scenarios. Share knowledge with the industry to help make everyone better at hunting evil.

ACCESS CONTROL

Get the proper permissions and network authorizations to perform incident response. It is important to have the organization add/remove permissions to accounts as it is needed to solve problems and to conduct a successful incident response.

PHASE 2 IDENTIFICATION

COMMUNICATION

Communication is vital in this phase because it is part of the initial detection of an incident. It is important for users to report unusual activity to the help desk and for the network operators to pay attention to alerts. Appropriate communication can make or break the incident response.

DETECTION

Determine if the unusual activity or alerts are an actual detection of an incident. This determination should be quick since the next phases are time sensitive.

THE 5W AND H

Determine who did what, when did they do it, why did it happen, where it occurred, and how. Not all of these will be discovered immediately but it is important to understand as much of the incident as soon as possible.

PHASE 3 CONTAINMENT

LIMIT THE DAMAGE

Limit the damage to the network and isolate the attack immediately. This is usually a short-term fix which should be remedied as soon as possible.

FORENSIC COPY

Create a forensic image of the affected systems with common tools in the forensic community. This preserves evidence of the incident to further investigate and prosecute if the incident was a result of criminal activity.

LONG TERM

Initially, temporary fixes are made in order to get the network back up. However, it is important to address long term containment needs to be addressed in case back doors have been left from attackers. This is important for the later phase of recovery.



PHASE 4 ERADICATION

REMOVAL


Remove the malicious content off the affected systems and ensure they are thoroughly cleaned.

RESTORATION

This includes reimaging of the systems hard drives from safe backups.

PREVENT REINFECTION

Improve defenses of the network by fixing vulnerabilities, keep systems updated, and disabling unnecessary permissions and services.



PHASE 5 RECOVERY

SET A PLAN

It is vital to make a final plan to completely restore operations. This decision should include the advice of the incident response team. The system operators and owners should set a time and date to conduct the recovery and how long the recovery will take.

RESTORE OPERATIONS

Carefully bring the affected systems back into the network. The key goal is to prevent another incident and not to reinfect the network of the issue which was just resolved.

VALIDATION

Test, monitor, and validate the affected systems are working properly prior, during, and after the restoration.

PHASE 6 LESSONS LEARNED

DOCUMENTATION

It is important to document the entire response process in order to learn from any positive and negative actions. The documentation should include anything not documented during the incident and to be completed in a report format. The report can be used as reference material in future incidents and onboarding of new team members.

MEETING

Team members should meet within 2 weeks of the end of incident response. The meeting should go over the initial detection, scope of the incident, how it was contained and eradicated, work performed during the recovery process, where the team was effective and areas in need of improvement.

SHARE WITH OTHERS

It is important to have time for suggestions and discussions between team members. Sharing of ideas and information is extremely beneficial to future effectiveness in future incident responses.

THANK YOU FOR YOUR TIME AND ATTENTION.

“...AS WE KNOW, THERE ARE KNOWN KNOWNs; THERE ARE THINGS WE KNOW WE KNOW. WE ALSO KNOW THERE ARE KNOWN UNKNOWNs; THAT IS TO SAY WE KNOW THERE ARE SOME THINGS WE DO NOT KNOW. BUT THERE ARE ALSO UNKNOWN UNKNOWNs, THE ONES WE DON'T KNOW WE DON'T KNOW.”

- US SECRETARY OF DEFENSE, DONALD RUMSFELD DURING A PENTAGON PRESS BRIEFING IN FEBRUARY 2002.

Presentation by James Nolen

nolenjgn@my.gvltec.edu