A QUICK PRIMER TO INCIDENT HANDLING / RESPONSE

NOT MEANT AS A SUBSTITUTE FOR PROPER TRAINING, BUT RATHER JUST TO CREATE INTEREST AND SHINE A LIGHT ON THE SUBJECT AREA

Derek Hill
@secureITtoday
derek@dh-solutions.com

PICERL

- Preparation – Plan for incidents, practice your plan
- Identification – How can we tell there is an incident vs. just an event
- Containment – Stop the bleeding, but don't kill the patient
- Eradication – Remove the adversary out of your network/systems
- Recovery – Getting back to business
- Lessons Learned – What happened, how can we get better at all of the above?

PREPARATION IS THE KEY TO SUCCESSFULLY DEALING WITH AN INCIDENT

- Get executive buy-in
  - You will need to have resources to create a plan and a lot more resources to execute a plan
  - Make sure you have documented authority during an incident, no need for politics or infighting during an incident
- Build a plan
  - How detailed the plan is will depend on the size of your organization
  - Create a list of roles and responsibilities, you don't need any infighting during an incident – update this as people change
  - Have an offline copy you can distribute in case the electronic version is not available or it has been compromised
- Establish external contracts (if needed) in advance
  - Incident response team
  - Others, such as public relations, legal, etc.
  - Make sure you have clear SLA, payment terms, timelines, etc. clearly documented

PREPARATION - CONTINUED

- Know your environment, have diagrams, critical systems lists, credentials (local and domain), data storage locations, etc.
- Enable logging on all your devices
  - You cannot use data you don't have
  - Centralized (remote) logging is more effective and harder to tamper with by the adversary
  - Log correlation via a SIEM is often a way an incident is detected
- Your team needs to know what to do during an incident
  - Make sure your staff is properly trained
  - Practice the plan, during an incident is not the place for people to learn about what they need to do
- Create a communications plan
  - Avoid using company systems email/phone during an incident, the adversary can be in your system and see all communication
  - Establish the communication stakeholders
- Define a war room, both physical and on-line
- Most important – Practice your plan, not just once, but on a regular basis

IDENTIFICATION
CAN YOU DETERMINE IF AN INCIDENT HAS OCCURRED

- Is it an event or an incident?
  - Look for correlating evidence
- Document everything meticulously
  - Create a timeline of when, who, what – this might need to be used in a criminal investigation and could become evidence. Even better if you have trained evidence handlers on your team (think preparation)
- Look for indicators of compromise (IOC)
- Determine severity, urgency and initial impact
- Review and take the appropriate actions based on your plan
  - This could include calling in outside resources previously retained, law enforcement, legal council, etc.
- Communicate to stakeholders

CONTAINMENT
STOP THE BLEEDING

- Implement the incident response playbook (plan) previous rehearsed
- Prevent further damage
  - Segregate affected systems onto their own VLAN/Network
- Determine the source, what was exploited (vulnerability)
- Conduct damage assessment – the scope
  - What was taken (ie. Confidential data, PII, PHI, financial data, intellectual property, etc.)
  - What was changed (ie. Files, DB records)
  - What was created (ie. Backdoors, user accounts)
- Acquire, but preserve any evidence (keep memory in tact, image disks)
  - Keep detailed notes as previously mentioned, this might become evidence in a future criminal proceeding
- Communicate to stakeholders

ERADICATION
REMOVE THE ADVERSARY AND THEIR TOOLS FROM YOUR SYSTEMS

- Eradicate the incident
  - Remove any indications of vulnerabilities
    - Keep in mind, that good adversaries cover their tracks and know how to hide, this will not be an easy task, be diligent, patient and thorough – you might have to do this repeatedly
    - You will most likely find additional systems where the adversary is present, but hasn't exploited yet, follow the same containment and eradication steps
  - Put safeguards in place to prevent reoccurrence of an infection
- Try to get a better understanding of the attack vector and take appropriate actions
- Document everything you do and preserve evidence
- Communicate to stakeholders

RECOVERY
GETTING BACK TO NORMAL

- Best course of action is to rebuild systems from scratch using known good media
    - Restore data either from backups or using out of band techniques such as portable drives. Do not put compromised systems back on the network – wipe the drives instead
        - Ensure that data removed from other systems has not been compromised
        - Check timestamps and hashes on files with known good values
    - Patch all systems, especially the same vulnerability on non affected systems
    - Slowly restore services, watch for abnormal behavior
        - This could indicate that not everything was contained (the same attack comes back)
        - Continue until full services are restored
    - Communicate to stakeholders

LESSONS LEARNED
WHAT WENT RIGHT, WHAT DIDN'T AND HOW CAN WE GET BETTER

- Try to conduct the Lessons Learned (After Action) session within 14 days if possible, while everything is still fresh but allow enough time to get back to normal
- Use the previously gathered notes to ensure no detail is left out/forgotten
  - Review the timeline
  - How was the incident detected, was is done in a reasonable amount of time
  - Who did what, when, why, how
  - How effective was their action
  - What could have been done better
  - Identify gaps
- Create a detailed report with the finding, including the areas for improvement
- Communicate to stakeholders
- Periodically follow up on the implementation of the areas for improvement

REFERENCES

- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- https://www.sans.org/reading-room/whitepapers/incident/
- https://www.cso.com.au/article/600455/six-stages-incident-response/
- https://www.sans.org/reading-room/whitepapers/incident/incident-handling-service-33289
- http://www.verizonenterprise.com/view/solnsbriefs/11411/threat-intel-and-response-services