# Response Strategies

INFO-6081 – Monitoring & Incident Response

FANSHAWE

# Learning Outcomes

- Incident Response Strategies
- Incident Containment
- Identifying Attacking Hosts
- Incident Eradication
- Incident Recovery
- Handling Incidents

# Incident Response Strategies

- Incident response strategies describe the actions taken by the CSIRT to regain control of compromised systems and restore operations to normal
- When the CSIRT is activated the first task they are charged with is an assessment of the current situation
  - The goal of this assessment is to determine the nature of the incident (if any), and to take steps to mitigate the effects of the incident
- The outputs of the detection and analysis phases serve as inputs for containment, eradication and recovery

# Incident Handling Checklist

| | Action | Completed |
|---|---|---|
| | **Detection and Analysis** | |
| 1. | Determine whether an incident has occurred | |
| 1.1 | Analyze the precursors and indicators | |
| 1.2 | Look for correlating information | |
| 1.3 | Perform research (e.g., search engines, knowledge base) | |
| 1.4 | As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence | |
| 2. | Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.) | |
| 3. | Report the incident to the appropriate internal personnel and external organizations | |
| | **Containment, Eradication, and Recovery** | |
| 4. | Acquire, preserve, secure, and document evidence | |

| | | |
|---|---|---|
| 5. | Contain the incident | |
| 6. | Eradicate the incident | |
| 6.1 | Identify and mitigate all vulnerabilities that were exploited | |
| 6.2 | Remove malware, inappropriate materials, and other components | |
| 6.3 | If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them | |
| 7. | Recover from the incident | |
| 7.1 | Return affected systems to an operationally ready state | |
| 7.2 | Confirm that the affected systems are functioning normally | |
| 7.3 | If necessary, implement additional monitoring to look for future related activity | |
| | **Post-Incident Activity** | |
| 8. | Create a follow-up report | |
| 9. | Hold a lessons learned meeting (mandatory for major incidents, optional otherwise) | |

# Incident Containment

- The first step of response is to contain the actions taken by the attacker
- Once containment is achieved, eradication and recovery can start
- Incident Containment describes the actions taken by the CSIRT to limit the scale and scope of the incident and to regain control over information systems
- The actions taken by the CSIRT will vary based on the nature of the attack, and may have an adverse effect on the ongoing operations of the organization

# Incident Containment

- Some examples of containment activities include:
    - Changing passwords of an affected account
    - Disabling an affected account or system
    - Disabling affected services
    - Shutting down a host
    - Disconnecting a host from the internet
    - Disconnection a host from the network
    - Restricting or deactivating part of the network
    - Disconnecting the network from the internet
    - Shutting down large sections of the network
- Some organizations may be uncomfortable with the severity of some of the previously describes actions

# Incident Containment

- Depending on the risk appetite of an organization, they may outline the type of incident containment that the CSIRT must follow
- If the organization simply wants to prevent future actions, containment is often a much simpler procedure
- If the organization wants to prosecute intruders, they may have a measure of acceptable loss, in order to “catch the intruder in the act”
- Open communication with the CIO or CSIO is critical before taking any actions that may affect the organization as a whole

# Identifying Attacking Hosts

- When the CSIRT is responding to a threat, it must identify the hosts that the attacker is using to infiltrate the network
- While it is often desirable to identify the attacker, this process is time consuming and most attackers will have taken measures to keep their true identities and locations hidden
- It is usually a better strategy to focus the response efforts on the containment, eradication and recovery of network resources and minimize the impact of the attack

# Identifying Attacking Hosts

- When identification of the attacker is necessary, the following activities can provide insight:
  - **Identification of the IP address of the attacking system**
    - The IP address of an attacker may reveal his location, or the service account used to conduct the attack
    - IP information is often unreliable due to VPNs, Tor and botnets
  - **Research the IP address of the attacker**
    - Researching the logged IP information could reveal information about similar attacks
  - **Incident/attack database search**
    - Searching event data in databases such as IDPS or firewalls may help diagnose the incident

# Incident Eradication

- Once the immediate containment of the incident is in place, the CISRT can move onto dealing with the contamination left behind on compromised hosts
- Attackers often leave a lot of damage in their wake, with successful attacks usually resulting in rootkits and other backdoors remaining on the affected systems
- Malware often results in damage that can affect a system long after the attacker has ceased their activities, or have been blocked by containment

# Incident Eradication

- Attackers may have modified the OS, system files or logs, user accounts, groups or user data
- All of the affected items must be identified, and restored to the state they were in before the incident
- Many practitioners believe that a compromised system can never truly be restored to a trusted state after an attack, and must be restored from a trusted backup, or rebuilt from known trusted media

# Concurrent Recurrence

- When working to contain an incident, the CSIRT must also prevent the attacker from initiating a new incident before the current one is resolved
- When a second attack occurs by means of the same technique, while the first attack is in progress, it is known as a concurrent recurrence
- The CSIRT must continuously monitor all assets (not just those associated with the current attack) that are still vulnerable using the same or similar attacks
- Concurrent recurrence does not always indicate an attack by the same individual, as the attacker may have shared the details of compromise

# Incident Recovery

- Incident recovery describes the steps required to return the organizations resources to a pre-incident state
- Incident recovery usually involves executing recovery operations and restoring systems from trusted backups
- One challenge of the recovery process is identifying data that may have been disclosed
- Corrupted data can be recovered, but disclosed data never will be
- If disclosed data affects external stakeholders, additional actions may be required

# Containment and Eradication Strategies

- The SCIRT is responsible for selecting the appropriate reaction strategy during containment and eradication, which can seem like an exercise in risk assessment
- The following details can affect this decision:
  - Type of attack
  - Method of incursion
  - Current/expected level of compromise
  - Current/expected level of loss
  - Targeted resources value and sensitivity
  - Legal or Regulatory impacts of a specific response

# Containment and Eradication Strategies

- The incident response planning process should have identified containment strategies for most major event types
- Each complete strategy should provide details on how to handle:
  - Theft or damage to assets
  - If evidence for a potential criminal investigation should be collected
  - Service-level commitments and contract requirements
  - Allocation of resources to activate the strategy
  - Graduated responses
  - Duration of containment efforts

# Handling Denial of Service (DoS) Incidents

- A denial of service occurs when an attacker prevents legitimate users of a service or system from accessing it
- Generally, denial of service attacks are made possible by overloading the resources of a system with more connections than that system was designed to handle
- Distributed denial of service attacks utilize multiple hosts to magnify the number of connections

# Handling Denial of Service (DoS) Incidents

**During the Attack:**

- Detect the attack
- Remove the attackers access
  - Disconnect the resource’s network connection
  - Block the source IP address on the perimeter firewall
  - Block the victim service on the perimeter firewall
  - Engage service provider
  - Relocate the target system

# Handling Denial of Service (DoS) Incidents

**After the Attack:**

- Decide if the organization will pursue the attacker criminally
- Remove filtering rules from perimeter firewall

**Before the Attack**

- Establish dialogue with service providers about procedures related to DoS incidents, contact numbers, expected traffic types and flows, etc.
- Implement prevention techniques such as IDPS and firewall rules for known attack types

# Handling Denial of Service (DoS) Incidents

- Monitor resources to determine when an attack is occurring
- Establish remote logging to record a transcript of events
- Implement elastic technologies such as rapid scaling to provide additional resources at higher than expected traffic peaks
- Partner with a content delivery network to provide multiple copies of critical resources located close to the main users of your service

# Handling Malware Incidents

- Malware is a generic term for software that is designed to attack, corrupt, disrupt, damage or provide unauthorized access to a system
- Malware can include worms, viruses, spyware, ransomware, adware, trojan horses, rootkits, logic bombs and more
- Sophisticated malware attacks often involve blended malware, which includes components of multiple different malware types

# Handling Malware Incidents

**During the Attack**

- Antivirus, anti-malware and IDPS are the frontline forms of detection when malware is concerned; however, users may also notice changes to their system
- Anti-malware and IDPS systems may automatically detect and contain the infection
- If the detection was not automatic, the CSIRT could take some of the following actions:
  - Scanning internal systems for unusual service ports
  - Analyzing network logs for anomalous items

# Handling Malware Incidents

  - Updating HIDS with up-to-date signature files
  - Auditing the system services for unauthorized entries
- Notify security application vendors of any newly discovered malware that infected a system without detection
- Add phishing based attacks to email filtering applications
- Block known attackers
- Temporarily quarantine new email
- Isolating hosts from the internet or peer

# Handling Malware Incidents

**After the Attack**

- After a malware attack it is crucial that systems are monitored for any signs of reinfection or alternate infection
- Report the attack to any required legal or compliance organizations
- Inform users of the incident

**Before an Attack**

- Provide training and awareness programs for users

# Handling Malware Incidents

- Review vendor and IR agency for postings related to common threats: CERT https://www.us-cert.gov/, SecurityFocus https://www.securityfocus.com/, Mitre https://www.mitre.org/
- Implement IDPS scanning
- Implement backup and recovery plans
- Use antimalware scanners
- Block distribution of executable extensions
- Minimize use of file transfer capabilities

# Handling Unauthorized Access Incidents

- Unauthorized access refers to any access attempt an individual or application makes to gain access to an information or asset it does not have permission of clearance to possess
- Examples of unauthorized access include:
  - Gaining unauthorized access to a network or computing resource, including port scanning and ping sweeping
  - Defacing or modification of any public-facing information systems such as the organizations website
  - Cracking passwords to gain access to restricted information systems

# Handling Unauthorized Access Incidents

  - Sniffing network traffic without express authorization
  - Using social engineering techniques to obtain access or information to restricted systems or networks

**During the Attack**

- Unauthorized access come in many forms, and as such requires many detection mechanisms
- Containments strategies include:
  - Isolate affected systems from the network
  - Disable affected ports or services

# Handling Unauthorized Access Incidents

- Filter the undesired traffic at the perimeter firewall
- Block the IP(s) that the attacker is using to connect to the network
- Disable affected user accounts and use a forced sign-out for systems that support this feature

**After the Attack**

- Identify the method the attacker used to gain entry and prevent future incursions
- Force a password reset for all affected accounts

# Handling Unauthorized Access Incidents

- Restore any affected data from a trusted backup

**Before the Attack**

- Implement industry accepted best practices
- Centralize authentication and authorization services
- Enforce an effective password policy that includes multiple factors
- Harden systems and devices against unauthorized access

# Handling Hybrid Incidents

- Many incidents are comprised of components from multiple incident types
- A malware infection could be the result of a phishing campaign, but it could be the result of an attacker operating on the network
- This requires the CSIRT to adapt their response strategies to contain and eradicate the various components of a hybrid attack
- CSIRT should prioritize components as they are uncovered, contain each incident and scan for others

# Summary

- Incident response strategies describe the actions taken by the CSIRT to regain control of compromised systems and restore operations to normal
- Incident containment limits the scale and scope of the incident and is used to regain control over information systems
- Identifying Attacking Hosts is a key component of response and necessary to contain an attack
- Incident Eradication takes steps to remove the compromised resources from the network
- Incident Recovery is used to return the organizations resources to a pre-incident state

# References

- Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology. doi: 10.6028/nist.sp.800-61r2
- Whitman, M. E., Mattord, H. J., & Green, A. (2014).  Chapter 7: Incident Response Strategies. Principles of incident response and disaster recovery (2nd ed.). Australia: Course Technology Cengage Learning.