Containment, Eradication, and Recovery

➢ Choosing a Containment Strategy

- ✓ Containment is important before an incident overwhelms resources or increases damage.
- ✓ Most incidents require containment, so that is an important consideration early in the course of handling each incident.
- ✓ Containment provides time for developing a tailored remediation strategy.
- ✓ An essential part of containment is decision-making (e.g., shut down a system, disconnect it from a network, disable certain functions).
- ✓ Such decisions are much easier to make if there are predetermined strategies and procedures for containing the incident.

Contd…

➢ Evidence Gathering and Handling

- ✓ Identifying information (e.g., the location, serial number, model number, hostname, media access control (MAC) addresses, and IP addresses of a computer)
- ✓ Name, title, and phone number of each individual who collected or handled the evidence during the investigation
- ✓ Time and date (including time zone) of each occurrence of evidence handling
- ✓ Locations where the evidence was stored.

Contd…

- ➢ Identifying the Attacking Hosts

- ✓ Validating the Attacking Host’s IP Address
- ✓ Researching the Attacking Host through Search Engines
- ✓ Using Incident Databases
- ✓ Monitoring Possible Attacker Communication Channels

Contd…

➢ Eradication and Recovery

- ✓ After an incident has been contained, eradication may be necessary to eliminate components of the incident, such as deleting malware and disabling breached user accounts, as well as identifying and mitigating all vulnerabilities that were exploited.
- ✓ During eradication, it is important to identify all affected hosts within the organization so that they can be remediated.
- ✓ In recovery, administrators restore systems to normal operation, confirm that the systems are functioning normally, and (if applicable) remediate vulnerabilities to prevent similar incidents.
- ✓ Recovery may involve such actions as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security (e.g., firewall rulesets, boundary router access control lists).

Post-Incident Activity

➢ Lessons Learned

- ✓ Exactly what happened, and at what times?
- ✓ How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
- ✓ What information was needed sooner?
- ✓ Were any steps or actions taken that might have inhibited the recovery?
- ✓ What would the staff and management do differently the next time a similar incident occurs?
- ✓ How could information sharing with other organizations have been improved?
- ✓ What corrective actions can prevent similar incidents in the future?
- ✓ What precursors or indicators should be watched for in the future to detect similar incidents?
- ✓ What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Contd…

- ➢ Using Collected Incident Data

- ✓ Number of Incidents Handled
- ✓ Time Per Incident
- ✓ Objective Assessment of Each Incident
- ✓ Subjective Assessment of Each Incident

Contd…

➢ Evidence Retention

- Organizations should establish policy for how long evidence from an incident should be retained.
- Most organizations choose to retain all evidence for months or years after the incident ends.
- The following factors should be considered during the policy creation:

✓ Prosecution

✓ Data Retention

✓ Cost

References

[1] https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf

[2] https://www.forcepoint.com/cyber-edu/incident-response

[3] https://digitalguardian.com/blog/what-incident-response

[4] https://www.drizgroup.com/driz_group_blog/7-steps-to-prioritize-cyber-security-threats-threat-remediation

[5]https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

Thank You !!!