INITIAL SECURITY INCIDENT QUESTIONNAIRE FOR RESPONDERS

Tips for assisting incident handlers in assessing the situation when responding to a qualified incident.

Understand the Incident's Background

What is the nature of the problem, as it has been observed so far?

How was the problem initially detected? When was it detected and by whom?

What security infrastructure components exist in the affected environment? (e.g., firewall, anti-virus, etc.)

What is the security posture of the affected IT infrastructure components? How recently, if ever, was it assessed for vulnerabilities?

What groups or organizations were affected by the incident? Are they aware of the incident?

Were other security incidents observed on the affected environment or the organization recently?

Define Communication Parameters

Which individuals are aware of the incident? What are their names and group or company affiliations?

Who is designated as the primary incident response coordinator?

Who is authorized to make business decisions regarding the affected operations? (This is often an executive.)

What mechanisms will the team to communicate when handling the incident? (e.g., email, phone conference, etc.) What encryption capabilities should be used?

What is the schedule of internal regular progress updates? Who is responsible for them?

What is the schedule of external regular progress updates? Who is responsible for leading them?

Who will conduct "in the field" examination of the affected IT infrastructure? Note their name, title, phone (mobile and office), and email details.

Who will interface with legal, executive, public relations, and other relevant internal teams?

Assess the Incident's Scope

What IT infrastructure components (servers, websites, networks, etc.) are directly affected by the incident?

What applications and data processes make use of the affected IT infrastructure components?

Are we aware of compliance or legal obligations tied to the incident? (e.g., PCI, breach notification laws, etc.)

What are the possible ingress and egress points for the affected environment?

What theories exist for how the initial compromise occurred?

Does the affected IT infrastructure pose any risk to other organizations?

Review the Initial Incident Survey's Results

What analysis actions were taken to during the initial survey when qualifying the incident?

What commands or tools were executed on the affected systems as part of the initial survey?

What measures were taken to contain the scope of the incident? (e.g., disconnected from the network)

What alerts were generated by the existing security infrastructure components? (e.g., IDS, anti-virus, etc.)

If logs were reviewed, what suspicious entries were found? What additional suspicious events or state information, was observed?

Prepare for Next Incident Response Steps

Does the affected group or organization have specific incident response instructions or guidelines?

Does the affected group or organization wish to proceed with live analysis, or does it wish to start formal forensic examination?

What tools are available to us for monitoring network or host-based activities in the affected environment?

What mechanisms exist to transfer files to and from the affected IT infrastructure components during the analysis? (e.g., network, USB, CD-ROM, etc.)

Where are the affected IT infrastructure components physically located?

What backup-restore capabilities are in place to assist in recovering from the incident?

What are the next steps for responding to this incident? (Who will do what and when?)

Key Incident Response Steps

1. Preparation: Gather and learn the necessary tools, become familiar with your environment.
2. Identification: Detect the incident, determine its scope, and involve the appropriate parties.
3. Containment: Contain the incident to minimize its effect on neighboring IT resources.
4. Eradication: Eliminate compromise artifacts, if necessary, on the path to recovery.
5. Recovery: Restore the system to normal operations, possibly via reinstall or backup.
6. Wrap-up: Document the incident's details, retail collected data, and discuss lessons learned.

Additional Incident Response References

Incident Survey Cheat Sheet for Server Administrators
http://zeltser.com/network-os-security/security-incident-survey-cheat-sheet.html

Windows Intrusion Discovery Cheat Sheet
http://sans.org/resources/winsacheatsheet.pdf

Checking Windows for Signs of Compromise
http://www.ucl.ac.uk/cert/win_intrusion.pdf

Linux Intrusion Discovery Cheat Sheet
http://sans.org/resources/linsacheatsheet.pdf

Checking Unix/Linux for Signs of Compromise
http://www.ucl.ac.uk/cert/nix_intrusion.pdf

Adapted by **Maynard Partners LLC -** www.maynardpartners.com - under Creative Commons v3 "Attribution" License. Authored by Lenny Zeltser.