Incident Response

May 2004

By Lawrence Allhands

BlueMotorcycle Consulting
650/740-4821
2830 Flores #18
San Mateo, CA 94403
http://www.bluemotorcycle.com
Abstract

“Titanic, name and thing, will stand as a monument and warning to human presumption”

_The Bishop of Winchester, preaching in Southampton, 1912._

Malicious hackers are everywhere today. Keeping them out of your network resources is of vital importance.

But what do you do when your network is compromised? How do you identify what areas have been compromised? Which machines are safe to use? Is your data protected? What steps are necessary to restore your network and its resources to normal?

This is where having an incident response plan in place for your network is vital. Whether your network consists of four computers or four hundred, you need to have a plan in place to respond effectively to network security breaches.

This paper will touch on some of the main areas of consideration when developing an incident response strategy.

The information in this paper complies with the guidelines of the Federal Computer Incident Response Center of the US Department of Homeland Security.
**Definitions/Figures**

**Phases of Incident Response**

<table>
<thead>
<tr>
<th>Phase 1 (Reaction)</th>
<th>Detection, Assessment, and Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase 2 (Restoration)</td>
<td>Containment, Evidence Collection, Analysis, Investigation, and Mitigation</td>
</tr>
<tr>
<td>Phase 3 (Resolution)</td>
<td>Remediation, Recovery, Debrief</td>
</tr>
</tbody>
</table>

**Phase 1 (Reaction) Steps**

- Establish Incident Response Leader
- Documentation
- Preserve Evidence
- Verify Incident
- Notification
- Determine Status
- Establish Goals
- Develop & Implement Plan
- End Phase 1

**Phase 2 (Restoration) Steps**

- Verify Containment
- Evaluate Phase 1
- Gather Evidence
- Analyze Evidence
- Develop Theories
- Mitigate Risk
- End Phase 2

**Phase 3 (Resolution) Steps**

- Report
- Archive Evidence
- Remediation
- Recovery
- Debrief
Incident Response

Phase 1 (Reaction)

Establish Incident Response Leader

Initially, the person discovering (recognizing) the incident should take the lead position until properly relieved by a trained Incident Response Team Leader. A detailed information turnover should be conducted upon the replacement of the Lead position if a replacement is deemed necessary.

The Incident Response Leader should coordinate the Phase 1 steps, documenting each step as they are successfully carried out.

Documentation

Second only to destruction or tainting of evidence, a lack of adequate documentation is the most common failure point in response to an incident. Initially, the proper organization of evidence is not nearly as important as is the thorough collection of ALL the information available.

Documentation can be electronic or handwritten; the focus should be to capture everything that occurs in detail, especially names, times, and events as they actually occurred (i.e. what, who, when, where, and why).

For the initial lead incident handler, a handwritten log may be adequate. In addition to handwritten written notes and log files, screenshots and digital pictures are valuable tools to capture information completely and unambiguously. Detailed documentation should continue throughout the entire incident.
**Incident Response**

**Preserve Evidence**
The point here is not necessarily to collect evidence, but rather to take steps to ensure its integrity and availability. We are primarily guarding against destruction of evidence through established processes like re-use of backup media, system use, or hard-disk wiping, and destruction or tainting of evidence through incident handling actions (logging on to affected systems, etc.).

Note that if deliberate evidence destruction is considered likely (e.g., by an insider), then more aggressive steps may be required to preserve evidence (i.e., physical evidence collection and safe storage may be required).

**Verify Incident**
Based on available data, establish whether or not an incident has actually occurred. Note that this must be done within the context of the previous steps, so actions such as logging on to affected systems, sending out broadcast emails, etc. should be avoided. Verification should result in one of three conclusion-action pairs: verified and proceed, undetermined and proceed, or refuted and conclude.

**Notification**
Once the incident validity is verified (or undetermined), the appropriate internal and external personnel should be notified immediately. There should be an established communications plan in place that will notify technical and management personnel, human resources, legal, public relations, and external entities (US-CIRC, local or federal law enforcement, etc.).
Incident Response

**Determine Status**

Determine whether the incident activity is actively occurring or ceased; if ceased, whether it is likely to resume.

Determine which and how many systems and data are actually or likely affected; also assess whether the incident activity has occurred solely within your domain, or whether external activity is involved (as a source or downstream target).

Consider what is at risk based on the incident activity. What is the likely impact of the data or systems have been affected? Are there other systems or data that have not yet been affected which are at risk?

**Establish Goals**

Establish the goals of the incident handling activity. Goals may include preserving reputation, protecting classified data, ensuring availability, etc. Satisfying all identified goals may not be practical or possible (for example, protecting data and ensuring availability are often incompatible).

Goals may also include taking steps to gather more information about a network intruder with a honeypot or fishbowl segment.

**Develop & Implement Plan**

Building off of the information available and the assessments in the prior steps, identify and evaluate options to meet the established goals. Develop a systematic plan to meet established goals. Execute plan; document the implementation and result of each step.

**End Phase 1**

At this point, we have ensured that evidence is preserved, initiated appropriate communications, have taken steps to contain the incident, and met our identified goals. The activities have likely been performed and supported by staff that have other responsibilities; so incident-handling responsibility can now be handed off to a dedicated investigation team.
Incident Response

Phase 2 (Restoration)

**Verify Containment**
Since the Phase 1 actions were most likely executed in a crisis environment, the first step in Phase 2 is to verify that the containment and related activities were effective.

**Evaluate Phase 1**
Review Phase 1 steps for thoroughness. Revisit of the scope, risks, and goals. Extended to include establishment of goals for current investigation team:

- How did the incident happen? When?
  - What is the verified scope or depth of the incident?
- Was there any activity after the initial incident?
- Who was the source of the attack?
- Immediate and future recommendations?

Establishing specific goals of the investigation may determine how to proceed (e.g., trap and trace, disconnect systems, active or passive searching, etc.).
Incident Response

**Gather Evidence**

Identify and capture any data relevant to the incident investigation. Evidence must be collected in such a way that the integrity of the evidence is ensured and a solid chain of custody is maintained.

All evidence relevant to the investigation must be captured; often this will include systems other than those directly affected by the incident (e.g., firewall logs, IDS logs, DHCP logs, mail servers, physical access logs, building sign-in sheets, surveillance video, etc.).

It is possible that some evidence collection activities may involve outside entities (e.g., ISPs, web hosting services, etc.); legal, HR, and other organization resources should be recruited as necessary to ensure that proper processes are followed.

A first round of evidence collection is usually followed by evidence analysis, theory development, and risk mitigation; Evidence collection activities will continue throughout these steps, especially as the investigation provides additional leads.

**Develop Theories**

Conducting evidence analysis is part science and part art. The success of the analysis and theory development will be highly dependent on the experience, tools, and knowledge of the investigation team.

The analysis will lead to the formulation of hypothetical answers to the questions identified in the Evaluation of Phase 1. Each theory must be substantiated by evidence, but the answers are often not absolute. Rather, the various evidentiary elements combine to indicate particular conclusions to greater or lesser degrees. It may be necessary to collect additional evidence, internal or external, to further support a given conclusion.
<table>
<thead>
<tr>
<th>Incident Response</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mitigate Risk</strong></td>
</tr>
<tr>
<td><strong>End phase 2</strong></td>
</tr>
<tr>
<td><strong>Phase 3 (Resolution)</strong></td>
</tr>
<tr>
<td><strong>Report</strong></td>
</tr>
<tr>
<td><strong>Archive Evidence</strong></td>
</tr>
<tr>
<td><strong>Remediation</strong></td>
</tr>
</tbody>
</table>
Incident Response

Recovery
If an incident has resulted in the destruction or corruption of data, then a recovery may be necessary. While partial or temporary recoveries may have been executed during the course of the incident handling process, it is only after the necessary remediation that a full and reliable recovery can be made.

Debrief
The final step of Phase 3 is a debrief to identify the strong and weak aspects of the exercise and to facilitate the communication of lessons-learned to other entities as appropriate.

About BlueMotorcycle Consulting
BlueMotorcycle is a systems integration and professional services consulting group conversant in high-quality, high-value, sensible technology solutions, specifically focused on networks, systems, security and specialized communications solutions. For more information, please call (650) 740-4821 or visit http://www.bluemotorcycle.com

© 2004 BlueMotorcycle, Inc. All rights reserved.