

Incident Response Part# 3: Containment

By Gregory S. Miles, Ph.D.

Last issue we looked at the critical, difficult step of identifying a computer security incident. This article is the third of a six part series in Incident Response (IR). IR professionals have adopted a basic core set of activities that encompass the IR discipline that includes IR preparation, identification, containment, eradication, recovery, and follow-up. Professional organizations that provide advice in the IR arena include but are not limited to the Carnegie Mellon Software Engineering Institute CERT[®] Coordination Center (www.cert.org), the SANS Institute (www.sans.org), CanCERT[™] in Canada (www.cancert.ca), and the Forum for Incident Response Security Teams (FIRST) (www.first.org). This article focuses on IR Containment.

The primary goal of the Incident Response Team is to maintain/restore business continuity, so containment of a security incident is vital. The purpose of containment is to limit the extent of an attack. The key elements of containment are decision-making and carrying out some predetermined steps.

The decision making process defines the critical steps that will be taken:

- Whether to shutdown a system
- Disconnect from a network
- Monitor system or network activity
- Set traps
- Disable certain functions (telnet, ftp etc)

Keep in mind that by removing access, you provide yourself denial of service and you also notify all users of the incident including potentially the person causing the problem. In some cases,

removing all access or functionality may be warranted, then restore normal operation in limited stages. In some

cases, it is worthwhile to risk some damage to the system if keeping the system up might enable you to identify an intruder.

It is critical during the containment stage to follow a predetermined set of procedures. Your organization or site should, for example, define acceptable risks in dealing with an incident, and should prescribe specific actions and strategies accordingly. This provides the opportunity for quick decisions to be made when needed. In the containment

“The primary goal of the Incident Response Team is to maintain/restore business continuity, so containment of a security incident is vital.”



stage of incident response, notification of appropriate authorities is critical.

Steps for Containment:

- Deploy containment team
- Secure area affected so no one accidentally starts changing things
- Review information from the identification phase
- Do not allow the system to be altered until a complete backup can be taken. Ideally this is a bit for bit image of the hard drives
- Avoid looking for the attacker by obvious methods
- Maintain standard procedures
- Consider planting “honey pots”
- Be cautious of compromised code (i.e. don’t log in as root or administrator on a potentially compromised machine still hooked to the network)
- Backup the system to forensically sterile media
- Store media in a safe location
- Acquire and review router and system logs
- Review logs from neighboring systems, especially if there is a trust relationship
- Determine the risk of continuing operations

- Keep system owners and administrators briefed on progress
- Never allow fault to be issued during the incident handling process
- CHANGE PASSWORDS and enforce a strong password policy
- Keep detailed records of every action taken

You cannot create a blanket set of systematic procedures to cover every organization since each organization and each operating system is different. Different risk factors will have to be set dependant upon the operations and function of the organization. Nevertheless, you can follow some basic procedures that keep you within the acceptable boundaries of action during containment. These parameters have to be set before an incident occurs; otherwise, there will be disorganization and confusion while trying to contain the incident. Clearly, Preparation (*see article: Incident Response Part 1: Preparation*) is still the most critical step in the incident response process.

Next IR article, we will be discussing Incident Response Part 4: Eradication.

© Security Horizon Inc. 2001

Dr. Miles is the COO/CFO for Security Horizon Inc and the Director of CyberCrime Response for JAWZ Inc. You can contact him at gmiles@securityhorizon.com.