

INTRODUCTION TO COMPUTER SECURITY INCIDENT HANDLING

BY TROY DEISINGER, CISSP, GCIH, GCUX, RHCT

What is security incident handling?

A security incident can be thought of as a violation, or imminent threat of violation, of computer security policies, acceptable use policies, or standard security practices (Grance 2-1).

Computer Security Incident Handling, commonly known as "Incident Handling" is the process of preparing for, detecting, containing, eradicating and recovering from security incidents.

The terms for each of these steps are defined as follows:

- **Preparation:** Steps taken to minimize the number of security incidents and formalize an organized response to a security incident.
- **Detection:** Steps taken to identify an event as a security incident.
- **Containment:** Steps taken to isolate the effects of a security incident.
- **Eradication:** Steps taken to remove the source of the security incident.
- **Recovery:** Steps taken to return the affected system(s) to normal operation.

As a final step, objectively review the incident after the fact, and use any knowledge gained to improve the process.

Why is security incident handling important to my organization?

Any device connected to a network will be attacked. Attacks are increasingly frequent, sophisticated and less obvious, often targeting the human components of system (HoneyNet 1).

Most organizations rely on the Internet to deliver their services, and are painfully aware that software often contains flaws that threaten their networked resources. Organizations commonly mitigate this threat by deploying a combination of Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Virus Detection Software, Malware Detection Software, Log Monitoring tools, etc. Unfortunately, unless the organization's security policies and procedures include systematic monitoring, and timely response to the output of these monitoring systems, none of these tools are effective.

Automated monitoring tools are also ineffective in mitigating attacks directed at the human element of the system. Human-focused attacks such as [social engineering](#) and [phishing](#) attempt to trick the people using a system into divulging sensitive system information. As automated security tools improve, so too will the number of human-focused attacks (HoneyNet 2). Organizations possessing policies and procedures including planned responses to these human-focused attacks, and conveying these responses to all members of the organization will be the most successful in minimizing their effect.

Increasingly consumers and the courts are holding organizations accountable for safeguarding sensitive client information (Rash). Minimizing the frequency and

severity of security incidents will reduce the risk of costly fines and the embarrassment associated with court cases.

Organizations must come to terms with the fact that security incidents are inevitable. Systematic, timely response to security incidents is imperative for successfully minimizing loss to both the client and the organization.

How do I get started?

The ultimate goal is an environment in which security incidents will be quickly identified, contained, and eradicated in a timely manner to minimize loss to the organization and the organization's clients.

To this end, the organization must develop and maintain security policies that clearly define the organizational efforts to protect its client data. Step-by-step security procedures define the enforcement of these policies. The security incident response process addresses the security policy requiring all security incidents be mitigated in a timely manner. Initial security awareness training should introduce the policies and procedures to all members of the organization. Subsequent regularly scheduled security awareness training sessions should provide follow-up, and introduce any updates or changes. The effectiveness of the security program hinges on its integration into the organizational culture. If the employees do not believe the policies and procedures are valid, they will not follow them.

Hiring and training personnel dedicated solely to security incident response would be ideal, but many organizations neither require, nor have the budget for such a staff. Fortunately, several on-line resources provide freely available, comprehensive information regarding security incident response. Organizations can use these resources to develop an appropriate security incident response methodology. Below are two examples:

National Institute of Standards and Technology: Computer Security Incident Handling Guide

<http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf>

Microsoft: Responding to IT Security Incidents

http://www.microsoft.com/technet/security/guidance/disasterrecovery/responding_sec_incidents.msp

Conclusion

Security incidents are virtually unavoidable. Successful attacks are costly to the organization and its clients. By developing a considered approach to securing network resources, and a prepared response to security incidents, an organization can thwart or minimize the effects of security incidents. Success depends entirely on the organization's commitment to cultivating a culture in which employees at all levels of the organization consider security incident prevention a priority.

Bibliography

Grance, Kent. Kim. "Computer Security Incident Handling Guide." NIST. Jan. 2004.
<http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf>

Rash. "Veterans Sue over Data Loss." Eweek. Jun. 2006
<http://www.eweek.com/article2/0,1895,1972946,00.asp>

"Know Your Enemy: Trends." Honeynet Project. 21 Dec. 2004.
<http://www.honeynet.org/papers/stats/>