



IT Security Presentation
Incident Response
October 16, 2002



Who I am

Adrien de Beaupré - IT Security Specialist
(ISC)_ CISSP
SANS GSEC and GCIH
7+ Years IT and Security Experience
Sit on the SANS GCIH advisory board,
authorized grader for SANS GIAC
Member of www.whitehats.ca



Incident Response

- The initial technical response to a computer network security incident
- Development of an Incident Response Plan
- There are 6 defined stages to incident response and handling
- Taken from the SANS publication:
Computer Security Incident Handling: Step-by-Step
Version 2.2 October 2001



Incidents

- What are incidents:
 - Malicious Code, Virus, Worm, Denial of Service, Espionage, Hoax, Network Probe, Unauthorized access, Cracking/Hacking
- Definition: an adverse event or a threat related to information security.



Developing IRP

- The steps involved in developing or refining the Incident Response Plan
- Includes:
 - Policy
 - Procedures
 - Reporting
 - Coordination
 - Law enforcement
 - Team membership
 - Decision making
 - Planning



Decisions

- Establish clear objectives
 - Investigate and forensic analysis
 - Contain and clean
- Roles and responsibilities
- Staffing and equipment requirements
- The rules of engagement
- Scope and constituency



Requirements

- Identify the processes, tools, policy and documentation required to successfully perform each of the tasks in the 6 steps of Incident Response
- Communications links and contact lists
- Plan the process of responding



Team

- Designate core team members
- Legal
- Human Resources / Personnel
- Public / Media Relations
- Security
- IT Technical staff
- Audit, investigations or forensics



Incident Response

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned / Follow up



Preparation

- Preparation: preparing the organization to respond to computer and network security incidents.
- Awareness: users and IT staff
- Procedures: responding quickly and correctly during crisis
- Training: knowing what to do
- Prevention



Preparation

- Prevent: keep patches and anti-virus DAT files up to date
- Keep aware and up to date on security incidents, vulnerabilities and issues
- Practice using tools and review procedures monthly
- Making sure you know who to call



Identification

- Is the event a security incident?
- If you know what should be there, you can identify what shouldn't be
- Locate problems early
- Tie intrusion detection and logs to IR
- Notify as soon as possible
- Stay calm, focus on handling the problem



Identification

- It is better to notify on a false alarm than to sit on your hands
- Never try to handle a situation by yourself, always contact and get help
- Get as much information about the problem as you can, and write it down
- Begin filling in incident reporting forms



Containment

- Contain the problem, disconnect the systems to prevent infection spreading
- Think carefully before you act
- Take notes of everything you see and everything you do
- Secure the area
- Forensic backup and evidence collection



Containment

- Email virus or worm: shut down the MTA
- On the network shut down the NIC or switch access, shut down the firewall
- May have to cut off an entire site
- It may be better to contain now than to wait and wonder
- The goal is to prevent further damage



Eradication

- Find out how the problem started and how it got in
- Remove the root cause of the problem, not just the symptoms
- Remove all traces of the malicious code
- Continue to log all actions



Eradication

- Locate a known good backup of the data on the infected system(s)
- If in doubt blow away the operating system and reload from scratch
- Improve the security of the system
- Prevent the same problem from reoccurring



Recovery

- Returning to normal
- Make absolutely certain the problem has been eradicated at all locations
- If necessary blow away and rebuild
- Be very careful re-introducing infections or vulnerabilities from restore of backup
- Monitor



Follow Up

- Lessons learned meeting and reports
- Retain your logs
- How can the problem be prevented in the future?
- How much did the incident cost to handle?
- Make recommendations to prepare for the next time.



Conclusion

- Incident response has to be quick
- Technical people have to know who to contact and what to do
- All actions must be coordinated
- Incident handling is NOT a solo sport



Questions?

© Elytra Enterprises Inc.



Resources

www.cert.org

www.sans.org

www.first.org

www.fedcirc.gov

www.ciac.org/ciac

www.cancert.ca

www.ocipep.gc.ca