Chapter 3

Incident Response Preparation

Ed Crowley

Spring 10

Topics

- Relevant IR Questions
- Pre-incident Preparation Overview
- Risk Identification
- Preparing Individual Hosts
- Secure Logging
- Host Defenses
- Network Prep
- Network Topology
- Establishing Appropriate Policies and Procedures
- Determining Response Stance
- Policies and Investigative Steps

Incident Preparation Goal

Create an infrastructure that provides rapid answers to questions arising after an incident. Including:

- What happened?
  - When did it start happening?
- What systems are affected?
- What information is compromised?
- Files created, modified, copied, or deleted?
- Who may have caused the incident?
- Who should be notified?
- What steps can be taken to rapidly recover to normal business procedures?

Pre-incident Preparation Overview

- Identify corporate risk
  - Info criticality matrix, vulnerabilities matrix, threat matrix
- Prepare hosts for incident response and recovery
- Prepare network by implementing network security measures
- Establish policies and procedures that facilitate incident response objectives.
- Create a CSIRT that can be assembled to handle incidents.
- Create a response toolkit for CSIRT use.

Risk Identification

A Critical IR Component

- Critical to do pre-incident preparation.
  - Understand big corporate security posture includes:
- What are the critical informational assets?
  - Information matrix
- What is their exposure?
  - Vulnerability matrix
- What are the relevant threats?
  - Threat matrix

Critical Asset Examples

- Confidential business information
- Nonpublic personally identifiable information
- Critical assets are assets that produce your organization's greatest liability, or potential loss.
  - Liability occurs through exposures.
- Corporate reputation

Preparing Individual Hosts

- Record cryptographic checksums for critical files
- Increase or enable secure audit logging
- Build up host defenses
- Back up critical data and store media securely
- Educate users about host based security

Integrity Process with Cryptographic Checksums

- To verify the integrity of files and data, the responder needs to compare the current system state against a “known good” system state.
- A cryptographic checksum, also known as a message digest or fingerprint, is basically a digital signature is used for the comparison

MD5

- Commonly accepted and used checksum today is MD5.
  - Created by Ron Rivest of MIT
  - Published April ‘92
  - RFC 1321.
- Creates a 128 bit checksum from any arbitrarily sized file.
- System baseline information should be securely stored offline.

Secure Logging

- By configuring log files, you can make them more complete and less likely to be corrupted.

Unix Logging

- Syslog is the heart of Unix log files.

Remote Unix Logging

Two steps

1. Create a central syslog server that accepts incoming syslog messages.
2. Configure other servers to log their messages to the syslog.conf file

- Process accounting then tracks the commands that each user executes.

Windows Logging

- Must be configured appropriately.
- By default, security auditing not enabled.
  - Individual audit options must also be configured.
- By default, Windows does not include remote logging capability.
- Often added with third party products

Application Logging

- Each application log must be configured differently.

General guidelines

- Log messages to a file that only the administrator can access
- Log messages to a secure, remote log host
- Log as much useful information as possible
- Log IP addresses rather than NetBIOS or domain names

Building up Host Defenses

- O/S and App software most recent version?
- Patched?
- Unnecessary services disabled?
- When faced with configuration choices, choose wisely.
- Access Control principle is that each user should have everything that they need and no more.

Back up Critical Data

- For Unix, the common backup utilities include dump, restore, tar, and dd.
  - Dump utility is the only one the preserves all three time/date stamps.
- Backups can be difficult to restore in a timely manner
- Depending on how the backups are created, they may not have accurate time of last access information.
- Back ups aren’t done until they have been tested.

User Education

- An important part of pre-incident preparation.

Network Prep

- Network monitoring, including logging, is essential.
  - There are many cases in which network monitors are the logical choice to hold accumulated evidence.
  - Appropriately configured firewalls
  - Appropriately configured ID systems
  - On routers, use appropriate access control lists
- Create/implement a network topology conductive to monitoring
- Where appropriate, encrypt network traffic
- Require authentication and SSO

Time

- In order to compare logs, all machines should utilize the same time. That is, they should be synchronized.
- Network time protocol.

Network Topology: Conductive to Monitoring?

- An accurate network topology map is useful in incident response
- While a network topology map generally gives a picture of the logical network layout, the topology map rarely shows host physical location and connectivity.
- Network monitoring must be supported by policies and procedures

Network Topology Attributes

Encryption

- SSL, SSH, VPNs
- Note, encrypting network traffic can also hinder the detection and investigation into any unauthorized or unlawful network based activity.

Authentication

- Both a host and network based security measure
- Kerberos, IP Security Protocol (IPSEC)

Establishing Appropriate Policies and Procedures

- Absolutely make or break an investigation
- Without any policies to the contrary, employees have an expectation of privacy.
- If you do not have explicit policies regarding an issue, information gathered in a search may or may not be admitted into court by a judge.

Determining Response Stance

- Before you begin to develop employees rules (AUP), you need to determine your stance on responding to incidents.

Potential Responses

- Ignore the incident
- Defend against further attacks
  - Identify and disable the initiators
- Perform surveillance and counterintelligence data gathering …

Factors Impacting Response

- Effect the incident has on business

Factors

- Legal issues and constraints
- Political influence or corporate politics
- Technical capabilities of the response team
- Funding and available resources

Business, Legal, and Political Issues

Business

- A tangible factor is lost business that occurred when site is unable to accept customers for a period of time.

Legal

- Prudent to consult legal counsel whenever administrative or judicial proceedings may be involved in the outcome.

Political

- Corporate politics will dictate the overall security philosophy.

Bottom Line

- Effective incident response requires good, hard-working, people who are technically savvy, aware of the corporate politics, knowledgeable about the business, and capable of reporting accurate, useful information to upper level management.

Policies and Investigative Steps

- Each of the response postures you may adopt needs to be supported by a corresponding policy.
- With appropriate acceptable use policies (AUPs), responsive legal advice, proper technical capabilities, and bannered systems, corporate investigators may be able to legally do things that law enforcement cannot do technically or cannot do without legal approval.

Trap and Trace

- A trap and trace captures network (header) traffic that does not include any user supplied content.

A trap and trace

- Protects network users privacy
- Permits system administrators to troubleshoot networks and locate source of technical problems.

Trap and Trace

- Policy permitting, corporate investigators can perform a trap and trace capture on their networks without a court order or subpoena.
- Note that no person may install or use a pen register or a trap and trace without first obtaining a court order unless:
  1. A service provider (organization) uses trap and trace monitors in the normal course of their business to ensure proper operation and use
  2. Or has user consent

Full Content Monitoring

- With proper system banners and AUPs, corporate investigators may be able to conduct full content monitoring and/or perform real time keystroke capturing.

Condition

- If the victim system is properly bannered, the intruder is one of the parties to the communication that has given prior consent.
  - If you can prove that the intruder saw the banner, he has implicitly consented to monitoring

Employee Machine Search

- 18 USC 2511-2521 applies to the interception of real time communications, not to access of stored communication.
- Access to stored communications is the reading or copying of data that is, at the moment it is being accessed, in storage.
- Access to stored communications is provided by 18 USC 2701--2709

Legal Differentiation

- The law differentiates between accessing unread mail and previously read mail
- The Fourth Amendment exception that is the most applicable to law enforcement and incident response teams is consent.
- A proper AUP can encompass employees consent to searching of their computer systems as a standard business practice

Policies Benefits

With appropriate policy, four pieces of information that corporate responders can obtain without the legal documentation necessary for law enforcement are:

1. Subscriber information
2. Transactional information
3. Electronic communications
4. Full content monitoring

Developing AUPs

- Security and incident response ground rules need to specify who is responsible for writing and updating policies as well as who is responsible for enforcing those policies.
- AUPs apply to everyone in an organization

Issues

- Decide who you trust
- Orient employees to the AUP
- Be consistent and clear in the AUP

Orientate Employees

- When policy is first developed, all current employees need to positively acknowledge its existence with a written signature, an orientation briefing or both.

- A policy that emphasizes involvement, rewards for incident notification, and security as a team effort will be more effective than the traditional “follow these five steps or die” approach.

Top Down AUP Design Issues

Technical

- Who can add and delete users?
- Who can access machines remotely?
- Who can scan your machines?
- Who can possess password files and audit (crack) them?
- Who gets root level access to what?
- Is posting to newsgroups allowed?
- Is Internet Relay Chat (IRC) or instant messenger permitted?
- Pirated software?

- Behavioral
- What web use is appropriate?
- How you will respond to sexual harassment, threats, and other inappropriate email messages?
- Who can monitor and when?
- Who can possess and use “hacker tools”?

AUP Design

- Design from the top down
- Contains both Technical and Behavioral attributes

Separate Policies

- Acceptable use policy
- User account policy
- Remote access policy
- Internet usage policy

- Procedures are the implementation of the policies of your organization

Creating a Response Toolkit

- Includes hardware, software, and documentation used during response.

Response Hardware

- Traditional brick or lunchbox configuration

Major hardware includes:

- Large hard drive
- SCSI card
- NIC
- Tape Drive
- Numerous drive related accessories.

See:

- www.forensic-computers.com

Response Software Kit

- Two to three native operating systems
- Selection of boot disks
- Access Data (FTK), Safeback, EnCase, DiskPro
- Disk write blocking utilities
- Multiple Disk Drivers
- Quick view Plus or similar
- An image of the complete setup on backup media

Network Monitoring Platform

- Robust with sufficient storage capacity

Documentation

- CSIRT must document all actions and findings.

Establishing an Incident Response Team

- After a possible computer security incident occurs, it is too late to assemble a team of experts to handle the incident.

Potential mission(s)

- Respond to all security incidents or suspected incidents using a organized formal investigative process.
- Conduct a complete bias free investigation
- Quickly confirm or dispel whether an intrusion or security incident actually occurred.
- Assess the incident's damage and scope

Potential Missions

- Establish a 24/7 hotline
- Control and contain incident
- Collect and document all incident related evidence
- Maintain chain of custody
- Select additional support when needed
- Protect privacy rights established by law or policy
- Provide liaison to proper LE
- Maintain appropriate confidentiality
- Provide expert testimony
- Provide management recommendations

Top Level Support

- Any policies, procedures, or incident response teams existing without toplevel support will usually fail.

- Training is also critical

Participate in professional organizations

- InfraGard
- High Technology Crime Investigation Association (HTCIA)
- Information Systems Security Association (ISSA)
- Forum of Incident Response and Security Teams (FIRST)

Questions?