Incident Response

denies it later on. ❑Harassment

❑Business Continuity Planning: deals with

❑Outage: Due to natural disasters, electrical

failures, … ❑Incident Response: deals with

❑Adverse events that threaten security.

❑CIA related incidents

❑Confidentiality

❑Integrity

❑Availability

❑Other Types

❑Reconnaissance Attacks

❑Repudiation : - Someone takes action and

Detection

- Extortion
- Pornography Traficking
- Organized Crime Activity

Countermeasures

deal with an incident.

- Subversion : - Bogus financial server
- Hoaxes
- Incident Response: Actions taken to

Rationale for Incident Response

- Abundance of Security-Related Vulnerabilities.
- Availability of Attack Systems and Networks.

- Actual and Potential Financial Loss
- Potential for Adverse Media Exposure
- Need for Efficiency
- Limitations in Intrusion Detection Capabilities.
- Legal Considerations
  - Due care.
  - Provisions of Law

Incident Response Architecture

- Policy
  - High-level description of essential elements of information security.
  - Do's and Don'ts for users and sys admins.
  - Sanctions for infractions.
  - Describes security stance of the organization.
    - Sanctioning of incident response capability: IR is a

required function of inform

Incident Response Risk Analysis

- No generally accepted methodology for assessing risks.

Criteria:

- Monetary costs.
- Operations impact.
- Public relations fallout.
- Impact on humans.

- Risk Categories:
- Break-in.
- Break-in in a single system at NASA delayed a launch.
- System was mission critical.
- Needed to be recertified before launch.
- Unauthorized execution of programs or commands.
- Privilege Escalation.
- Exploitation of CGI
- Web servers have frequently cgi scripts installed for demonstration purposes. These have known weaknesses.

Incident Response Risk Analysis

- Denial of Service attacks

- Web Defacement
- Virus and worm attacks
- Malicious active content
- Back door attacks
- Spoofing, Session tampering, hijacking, replay
- Determining Risk Probabilities
- Collect data within the organization.
- Collect data by other organizations.
- CERT Coordinating Center
- National Infrastructure Protection Center NPIC
- Vulnerability Analysis

- CERT, ALLDAS, ANTIONLINE 30

Incident Response Methodology

- Structure and Organization
  - Incidents create pandemonium
  - Incidents occur in bursts
- Efficiency
- Facilitates the process of responding to incidents.
- Facilitates dealing with the unexpected.
- Legal Considerations.

- Preparation
  - Setting up a reasonable set of defenses and controls based on threads.
  - Creating a set of procedures to deal with the incident efficiently.
  - Obtaining the resources and personnel to deal with the problem.
  - Establish an infrastructure to support incident response activity.

Incident Response Methodology

- Detection
  - Intrusion Detection Systems

- Detection Software & Reporting
- Containment: Strategies
  - Shutting down a system
  - Disconnect from the network
  - Change filtering rules of firewalls
  - Disabling or deleting compromised accounts
  - Increasing monitoring levels
  - Setting traps
  - Striking back at the attacker's system ☹
- Adhering to containment procedures.
  - Record all actions
  - Define acceptable risks in advance

❑Eradication: Eliminate the cause of the incident.

❑Software available for most virus, worm attacks. Procedures are very important. 32

Incident Response Methodology

❑Eradication in UNIX System

- Check .forward for unauthorized entries
- Use ps to find stray processes
- Ensure that essential files are not modified
- /etc/exports
- .login
- .logout
- .profile
- /etc/profile
- .cshrc
- /etc/rc directory
- .rhosts
- /etc/hosts.equiv
- at
- Examine system commands for changes

- netstat
- ls
- sum
- find
- diff
- /etc/nsswitch.conf
- /etc/resolv.conf
- /var/spool/cron
- kerb.conf

Incident Response Methodology

❑Eradication in UNIX System

- Discover real modification times for files
- Discover suid programs
- Ensure that all password files are the same

- Ensure that there are no unauthorized entries in the .rhost files
- Ensure that there are no unauthorized services running
- Search for all files created or modified during the time of the attack.
- Use the strings command to inspect binaries for clear text that might indicate mischief

Incident Response Methodology

❑ Eradication in Window System

- Ensure that the following have not been modified

- Security Accounts Manager (SAM) Database
- Services
- All .dll files
- Dial-in settings
- User manager for domain settings
- All logon scripts
- The integrity of all registry keys and values below Winlogon and LSA in the registry.
- Run entries in registry.
- Membership in all privileged groups.
- System and user profiles.

Incident Response

Methodology

- Eradication in Windows 2000

- Ensure that the following have not been modified
- Security Accounts Manager (SAM) Database
- Services
- All .dll files
- Scheduler
- Policy settings.
- Membership in privileged groups
- All logon scripts
- All security options
- All permissions for Active Directory.
- All DNS settings.
- Registry keys and values under Winlogon and Run in the registry. - Permissions and ownerships in \%systemroot%\ntds …

Incident Response Methodology

- Recovery: Return compromised systems back to its normal mission status.
- Recovery procedures: Safest is:
- Full rebuilt for system files.
- Restore data from last backup.
- Record every action.
- Keep users aware of status.
- Advise appropriate people of major developments that

might affect them.

- Adhere to policy regarding media contact.
- Return logging to normal level.
- Install patches for any exploited vulnerability.

Incident Response Methodology

- Follow-Up
  - Perform a post mortem analysis on each significant incident.
    - Exact description and timeline.
    - Adequacy of staff response.
    - What information was needed at what time.

- What would the staff do differently.
- How was interaction with management.
- What was the damage?

- Use for legal reasons: forensically sound evidence.
- Includes monetary damage.

- Reevaluation and modification of staff response.
  - Example: Break-in at Human Genome database.
  - Nobody knew who had called when more info was needed.
  - Gap in procedure was remedied during follow-up.

- Summary

1.Methodology is needed to deal with quickly evolving, chaotic situations. 2.Takes time to implement and to learn. Use mock events for training. 3. Stages flow into each other. 4. Methodology needs to be tailored to situation. 5.Follow-up needed to improve and adapt methodology.

Incident Response

Forming and Managing an IR-Team

- Incident response team vs. incident handlers
- Reasons for outsourcing:
  - Specialists can maintain and add to a complex skill set.
  - Specialists can charge for service.
  - Company might lack resources.
  - Small organizations do not need a team.

- Reasons for in-house incident response:
  - Sensitive data is better handled by employees.
  - In house team responds better to corporate culture.

Incident Response
Why an incident team?

- Expertise.
- Efficiency.

- ❑Ability to work proactively.
- ❑Ability to meet agency or corporate requirements.
- ❑Teams serve as liaison.
- ❑Ability to deal with institutional barriers.

Incident Response Basic Requirements

❑Control over incidents:

❑Full control over incident and data / resources involved **or** Control sharing **or** Advisory role.

❑Interagency / corporation coordination / liaison ❑ Clearinghouse

❑Contingency planning and business continuity services ❑ Information security development

❑Incident response planning and analysis

❑Training and awareness

Incident Response:
Determining / Dealing with Constituency

- Identify constituency
- Sys Ads are different than general user population
- Failure of dealing adequately with constituency leads to long term failure
- Failures:
  - Not getting back to an incident reporter.
  - Spreading misinformation.
  - Becoming too intrusive.

- Causing embarrassment or leaking information without authorization.
- Betrayal. 42

Incident Response: Success Metrics

- Good security No incidents.
- Makes success metrics difficult:
- Nr. of incidents
- Estimated financial loss.
- Self-evaluation / questionnaires
- Written or verbal reports by constituency
- Average time and manpower per incident
- Documentation by team members
- Awards / other forms of external recognition

Incident Response:

Organization of IR Team

- ❑Training the team
- ❑Mentoring
- ❑Self-Study
- ❑Courses
- ❑Library
- ❑Exercises
- ❑Testing the team / procedure
- ❑Dealing with resistance
- ❑Budget: not a revenue source, hard to quantify impact ❑Management reluctance
- ❑Organizational resistance: rival organizations, turf warfare ❑Internal politics
- ❑User awareness

Incident Response:

Organization of IR Team

- External Coordination
- Law Enforcement
- Media
- Other Incident Response Teams
- Infraguard
- Managing Incidents
- Bursty load: surviving the long haul
- Assigning incident ownership
- Tracking charts
- Priorization

Incident Response: Role of Computer

Forensics

- Determines policies:
- Ethical boundaries of response
- Legal boundaries of response
- To protect right's of insiders and outsiders
- To preserve evidence as legal evidence
- Rules for thorough documentation
- Protect evidence against accidental or intentional tampering / destruction
- Technical Response
- How to document
- How to establish chain of custody
- How to gather all possibly important evidence