Preparation for Incident Response

Preparation for IR

- Incident preparation provides rapid answers to the questions that will be asked *after an incident occurs:*
  - What exactly happened?
  - What system(s) was affected by the incident?
  - What information was compromised?
  - What files were created, modified, copied, or deleted?
  - Who may have caused the incident?
  - Who should you notify?
  - What steps can you take to rapidly recover to normal business procedures?

Three Areas of Preparation

- Preparing the organization
- Preparing the IR team
- Preparing the infrastructure

IDENTIFYING RISK

- **What are your critical assets?**
- **What is their exposure?**
- **What is the threat?**

- Identify and prioritize the risk
- Ensure that you spend resources preparing for the incidents most likely to affect your business

IDENTIFYING RISK

- **What are your critical assets?**
  - Produce the greatest liability, or potential loss
  - Organizations assets
    - Corporate reputation
    - Confidential business information
- **What is their exposure?**
  - people, processes, or technology result in or contribute to loss
  - unpatched web servers, Internet-facing systems, untrained employees, and lack of logging
- **What is the threat?**
  - Anyone connected to the Internet?
  - Anyone with physical access to a corporate building?
  - Only individuals physically within a secure area?

Preparing individual hosts

- **Record cryptographic checksums of critical files**
  - Use MD5 , use scripting language to automate this process (Tripwire package)
- **Increase or enable secure audit logging**
  - operating system and applications need significant logging
- **Build up your host's defenses**
  - If host is completely secure, many security incidents would be avoided
  - Three cornerstones of secure hosts:
    - Make sure that all operating system and application software is the most recent. Use the latest release and make sure that all patches, hot fixes, and updates are installed
    - Disable unnecessary services. If you are not using an application or network service, it should not be running. Unnecessary services introduce unnecessary risk
    - When faced with configuration choices, choose wisely. Many security exposures are introduced through sloppy system administration

Preparing individual hosts

- **Back up critical data and store media securely**
  - Take regular, complete system backups
  - Backups allow you to figure out what was modified, deleted, added,
  - Some backups save time/date information, which may be useful for checking the times files and directories were last accessed, modified, or created
  - Disadvantages:
    - Difficult to find a system to restore
    - backup may be taken after compromise,
    - may not have accurate time-of-last-access

Preparing individual hosts

- **Educate users about host-based security**
  - Users play a critical role in your overall security
  - Users should know what types of actions they should and should not take
  - should know the danger inherent in networking software installed by users
  - Users should be educated about the proper response to suspected incidents
    - immediately notify a designated contact
    - to take *no investigative actions, because these actions can often destroy evidence*
    - Make timely response

Preparing individual hosts

- These steps are not a one-time function
- Since hosts change over time with new users, software, and network configuration, these host preparation steps are best incorporated into organizational policies and procedures

Preparing a Network

- Network-based security measures are to be consider
- Network administrators play a critical role during incident response
- Network-based logging is absolutely essential - only hope to accumulate evidence.
- Network administrators are responsible for
  - the network architecture and topology
  - Devices like firewalls, routers, and intrusion detection systems
  - Reconfiguring these devices to block certain traffic during incident response

Preparing a Network

- Network security actions include the following:
  - **Install firewalls and intrusion detection systems**
    - Configure - simply to protect network, as well as to log activities
    - May decide to deny certain attacks and not log, or permit attacks and log in detail to learn more about the attacker
  - **Use access control lists on routers**
    - Access control lists (ACLs) allow certain types of traffic while prohibiting potentially dangerous traffic
  - **Create a network topology conducive to monitoring**
    - In the event of an incident, you must know the network topology in order to determine the best response strategy
  - **Encrypt network traffic**
    - enhances the security of any network - SSL,VPN, SSH
    - When attackers use encrypted protocols to access your systems, network monitoring and IDS systems are useless.
  - **Require authentication**
    - Authentication is both a host-based and network-based security measure
    - Usernames and passwords are often guessed easily
    - Using additional authentication—Kerberos, IP Security Protocol

ESTABLISHING APPROPRIATE POLICIES AND PROCEDURES

- Absent a proper policy, you may not be able to legally monitor
- Without any policies employees have an expectation of privacy
  - You cannot monitor their daily activities, peruse their email, observe their web-browsing habits, access their voice-mail systems, or review the contents of their computer system whenever you feel like it
  - Insiders may be emailing your vital trade secrets to your competitors, and hackers may be holding an electronic cocktail party on your networks their activities

ESTABLISHING APPROPRIATE POLICIES AND PROCEDURES

- With some preparation, planning, proper policies, and in-place procedures,
- We can determine when to respond to an incident
- We can also take the rights to monitor the activities of employees or unauthorized intruders

ESTABLISHING APPROPRIATE POLICIES AND PROCEDURES

- **Determining Your Response Stance**
  - need to determine your stance on responding to incidents
  - When an organization is the victim of a computer intrusion, denial-of-service (DoS) attack, insider theft of intellectual property, or other network-based computer crime, the organization can respond in several different ways:
    - Ignore the incident altogether.
    - Defend against further attacks.
    - Defend against further attacks by identifying and disabling the initiators (bycriminal arrest or civil action).
    - Perform surveillance and counterintelligence data gathering.

ESTABLISHING APPROPRIATE POLICIES AND PROCEDURES

- five factors that will influence how you respond to computer security incidents:
  - The effect the incident has on your business
  - Legal issues and constraints
  - Political influence or corporate politics
  - Technical capabilities of the response team
  - Funding and available resources

ESTABLISHING APPROPRIATE POLICIES AND PROCEDURES

- **Considering Business Issues**
  - e-commerce web site gets hacked and defaced
  - fixes the site first
  - secure the system by patching any security holes
  - damage to the victim is
    - unable to accept customers for a period of time
    - Organization lose reputation

ESTABLISHING APPROPRIATE POLICIES AND PROCEDURES

- **Benefits of Sound Policies**
  - Four pieces of information that corporate responders can obtain without the legal documentation and headaches that may be necessary for law enforcement personnel to endure
    - **Subscriber information**
    - **Transactional information**
    - **Electronic communications**
    - **Full-content monitoring**

ESTABLISHING APPROPRIATE POLICIES AND PROCEDURES

- **Developing Acceptable Use Policies (AUP)**
  - Decide whom you trust on your network.
    - monitor on-site employees as well as individuals using remote-access services.
    - determine whether you will monitor all activities or just a few select ones. Or monitor only after suspect
    - control and regulate employee behavior.
  - Orient employees to the AUPs.
    - advertised throughout the corporation and incorporated into new employee orientation.
    - employees will need to positively acknowledge - written signature
    - Provide refresher overview course on policies when major changes are made to policies.
  - Be consistent and clear in your AUPs.

ESTABLISHING APPROPRIATE POLICIES AND PROCEDURES

- **Developing Acceptable Use Policies (AUP)**
- **Before developing policies first** decide who is responsible for writing and updating the policies, as well as who should enforce those policies.
- AUPs affect everyone in an organization: the users, managers, internal auditors, legal staff, system administrators, and technical staff. Therefore, each group affected by the policy should be part of its approval process

ESTABLISHING APPROPRIATE POLICIES AND PROCEDURES

- **Designing AUP**
  - Be consistent and clear in your AUPs.

Designing from the Top Down

and use “hacker tools”?

- Technical

Who can add and delete users?

Who can access machines remotely?

Who can scan your machines?

Who can possess password files and crack them?

Who gets root-level access to what?

Is posting to newsgroups allowed?

Is Internet Relay Chat (IRC) or instant messenger permitted?

Will you condone use of 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”?

ESTABLISHING APPROPRIATE POLICIES AND PROCEDURES

- **Creating Separate Policies**
  - create a few smaller policy documents rather than to produce one enormous AUP
  - **Acceptable Use Policy**
    - Governs what behaviour is expected by each user
  - **User Account Policy**
    - Dictates how accounts are added to systems, who has root-level access, and even establish controls of where and when users can access prized resources
  - **Remote Access Policy**
    - Establishes who can access your systems remotely and how they can access those systems.
  - **Internet Usage Policy**
    - Covers how and when users can use the Internet, which is often a frequent source of misunderstanding between employers and employees.

ESTABLISHING APPROPRIATE POLICIES AND PROCEDURES

- **Developing Incident Response Procedures**
- Procedures are the implementation of the policies of your organization.

ESTABLISHING AN INCIDENT RESPONSE TEAM

- **Deciding on the Team's Mission**
- **Training the Team**
  - The mission of your CIRT may be to achieve all or most of the following:
    - Respond to all security incidents or suspected incidents using an organized, formal investigative process.
    - Conduct a complete investigation free from bias (well, as much as possible).
    - Quickly confirm or dispel whether an intrusion or security incident actually occurred.
    - Assess the damage and scope of an incident.

ESTABLISHING AN INCIDENT RESPONSE TEAM

- **Deciding on the Team's Mission**
  - Establish a 24-hour, 7-day-a-week hotline for clients during the duration of the investigation.
  - Control and contain the incident.
  - Collect and document all evidence related to an incident.
  - Maintain a chain of custody (protect the evidence after collection).
  - Select additional support when needed.
  - Protect privacy rights established by law and/or corporate policy.
  - Provide liaison to proper law enforcement and legal authorities.
  - Maintain appropriate confidentiality of the incident to protect the organization from unnecessary exposure.
  - Provide expert testimony.
  - Provide management