March 2008

INFORMATION TECHNOLOGY LABORATORY

Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

HANDLING COMPUTER SECURITY INCIDENTS: NIST ISSUES UPDATED GUIDELINES

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

Today, organizations that operate and manage information technology (IT) systems are spending more time than ever before in responding to security incidents. New incidents and threats that arise daily have the potential to seriously damage and disrupt the security of the organization's information and IT systems.

Security incidents are violations or threats of violation of the organization's computer security policies, acceptable use policies, or standard computer security practices. Organizations should consider carefully their ability to handle these security incidents and threats effectively when they plan, develop, and implement their IT security programs.

Applying risk management procedures, organizations should identify and assess the risks of security incidents and identify effective ways to deal with them. The first approach is to prevent security incidents whenever possible. But since not all incidents can be prevented, organizations should take steps to establish an incident response capability for rapidly detecting incidents, minimizing loss and destruction, identifying any weaknesses in their systems that may have been exploited, and restoring IT services. This is a complex undertaking, requiring considerable planning and the commitment of resources to carry out the plans.

Intrusion detection and prevention systems (IDPSs) and other mechanisms can be used to monitor threats. Clear procedures are needed to assess the current and potential impact of incidents and to implement effective methods for collecting, analyzing, and reporting data. Specific communication channels should be established with internal groups, such as human resources and legal staffs, and with external groups, such as law enforcement, the media, and other incident response teams.

Security Threats to IT Systems

The many security-related threats that organizations must address include:

- **Denial of Service (DoS)**—an attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.
- **Malicious Code**—a virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host.
- **Unauthorized Access**—a person gains logical or physical access without permission to a network, system, application, data, or other IT resource.

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. Bulletins are issued on an as-needed basis and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since February 2007:

- *Intrusion Detection and Prevention Systems, February 2007*
- *Improving the Security of Electronic Mail: Updated Guidelines Issued by NIST, March 2007*
- *Securing Wireless Networks, April 2007*
- *Securing Radio Frequency Identification (RFID) Systems, May 2007*
- *Forensic Techniques for Cell Phones, June 2007*
- *Border Gateway Protocol Security, July 2007*
- *Secure Web Services, August 2007*
- *The Common Vulnerability Scoring System, October 2007*
- *Using Storage Encryption Technologies to Protect End User Devices, November 2007*
- *Securing External Computers and Other Devices Used by Teleworkers, December 2007*
- *Secure Web Servers: Protecting Web Sites that are Accessed by the Public, January 2008*
- *Federal Desktop Core Configuration (FDCC): Improving Security for Windows Desktop Operating Systems, February 2008*

- **Inappropriate Usage**—a person violates acceptable use of any network or computer policies.
- **Multiple Component**—a single incident that encompasses two or more incidents; for example, a malicious code infection leads to unauthorized access to a host, which is then used to gain unauthorized access to additional hosts.

Updated Guide on Handling Security Incidents

NIST's Information Technology Laboratory recently issued NIST Special Publication (SP) 800-61 Revision 1, *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology*. Written by Karen Scarfone and Tim Grance of NIST and by Kelly Masone of Booz Allen Hamilton, NIST SP 800-61 Revision 1 provides practical guidance to help organizations establish an effective incident response program, analyze and respond to information security incidents, and reduce the risks of future incidents. The recommendations in the guide are useful for those organizations that are just setting up their incident handling teams, as well as those that have already done so.

The updated guide, which replaces NIST SP 800-61, *Computer Security Incident Handling Guide*, focuses primarily on the procedures and solutions for detecting, analyzing, prioritizing, and handling incidents. The guidelines and recommended solutions can be used on many different hardware platforms, operating systems, protocols, or applications and can be tailored to meet the specific security and mission requirements of different organizations.

NIST SP 800-61 Revision 1 provides in-depth information on the need for incident response capabilities. It covers the structures of incident response teams and discusses the other groups within an organization that might participate in incident handling activities. The basic steps of handling incidents effectively, including incident detection, analysis, containment, eradication, and recovery, are presented. Separate sections in the guide provide specific recommendations for handling the five types of incidents: denial of service (DoS), malicious code, unauthorized access, inappropriate usage, and multiple component incidents. All of these incidents are defined, and examples of each are given. The preparation, detection, analysis, containment, eradication, and recovery steps for each type of incident are detailed. Checklists for handling each of the five types of incidents are included.

The appendices bring together useful information sources that assist organizations in their incident handling programs. Included are a consolidated list of the recommendations that are discussed in the guide, incident response scenarios, and questions for use in incident response exercises. Also provided are suggested items of information to be collected about each incident, a glossary, an acronym list, lists of in-print resources, online tools, and other resources that help organizations in planning and performing incident response activities. In addition, the appendices present frequently asked questions about incident response activities and the steps to be followed in incident handling. The final section of the appendices contains incident reporting guidelines for federal agencies from the United States Computer Emergency Readiness Team (US-CERT) in the Department of Homeland Security.

This ITL bulletin summarizes the updated guide, which is available at:

http://csrc.nist.gov/publications/PubsSPs.html.

Basics of Incident Handling

Organizations face major decisions and actions when they develop their computer security incident response capabilities (CSIRC). One of the first considerations should be to create an organization-specific definition of the term "incident" so that the scope of the term is clear. The organization should decide what services the incident response team should provide, consider which team structures and models can provide those services, and select and implement one or more incident response teams. An incident response plan, and associated policies and procedures, should be developed when a team is established so that the incident response process is performed effectively, efficiently, and consistently. The plan, policies, and procedures should identify the team's interactions with other teams within the organization as well as with external parties.

The incident response process is composed of several phases. The initial phase involves establishing and training an incident response team, and acquiring the necessary tools and resources to enable the team to carry out its responsibilities. During this preparation activity, the organization also attempts to limit the number of incidents that will occur by selecting and implementing a set of controls based on the results of risk assessments. However, residual risk will inevitably persist after controls are implemented, and no control is foolproof.

The next phase is detection and analysis of security breaches, which alerts the organization whenever incidents occur. A

containment/eradication/recovery phase follows. Depending upon the severity of the incident, the organization can act to mitigate the impact of the incident by containing it and ultimately recovering from it. After the incident is adequately handled, the organization issues a report that details the cause and cost of the incident and the steps the organization should take to prevent future incidents. This last phase is post-incident activity.

The organization's incident response team should be available for contact by anyone who discovers or suspects that an incident involving the organization has occurred. One or more team members, depending on the magnitude of the incident and availability of personnel, should handle the incident. The incident handlers analyze the incident data, determine the impact of the incident, and act appropriately to limit the damage to the organization and restore normal services. Although the incident response team may have only a few members, the team's success depends on the participation and cooperation of individuals throughout the organization.

NIST Recommendations for Handling Security Incidents

NIST advises that organizations implement the following recommendations in planning and developing their incident response capabilities:

Establish and operate a formal incident response capability.

Federal agencies and departments are specifically directed to establish incident response capabilities under the Federal Information Security Management Act (FISMA) of 2002. Federal organizations are required to develop and implement procedures for detecting, reporting, and responding to security incidents. Federal civilian agencies are responsible for designating a primary and secondary point of contact (POC) to report all incidents to the United States Computer Emergency Readiness Team (US-CERT) and for documenting corrective actions that have been taken and their impact. Each agency is responsible for determining specific ways in which these requirements are to be met.

Also, policy guidance issued by the Office of Management and Budget (OMB) requires that agencies have a capability to provide help to users when security incidents occur in their systems and to share information concerning common vulnerabilities and threats (OMB Circular No. A-130, Appendix III). OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, provides guidance on reporting security incidents that involve personally identifiable information.

Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*, specifies minimum security requirements for federal information and information systems, including incident response. The specific requirements for the implementation of security controls are defined in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*.

Organizations should take the following steps in establishing an incident response capability:

- Create an incident response policy and plan;
- Develop procedures for performing incident handling and reporting, based on the incident response policy;
- Set guidelines for communicating with outside parties regarding incidents;
- Select a team structure and staffing model;
- Establish relationships between the incident response team and other groups, both internal to and external to the organization;
- Determine the services that the incident response team should provide; and
- Staff the incident response team and provide staff members with appropriate training.

Reduce the frequency of incidents by effectively securing networks, systems, and applications.

It is less costly and more effective to prevent incidents than to try to fix the problems that occur when security controls are inadequate. Many security incidents can overwhelm the resources and capacity of the organization to respond, and can result in delayed or incomplete recovery. Extensive damage may occur, and systems and information may not be available for long periods. When the security of networks, systems, and applications is effectively protected and maintained,

the incident response team can focus on handling serious problems.

Document the organization's guidelines for interactions with other organizations regarding incidents.

Clear procedures should be established to guide incident handling team members who may need to communicate with outside parties, including other incident response teams, law enforcement, the media, vendors, and external victims. These communications often must occur quickly, and guidelines are needed so that only the appropriate information is shared with the right parties. The inappropriate release of sensitive information can lead to greater disruption and financial loss than the incident itself. Creating and maintaining a list of internal and external POCs, along with backups for each contact, can help organizations to make the communications among the involved parties easier and faster.

Emphasize the importance of incident detection and analysis throughout the organization.

Organizations might experience thousands or millions of possible indications of security incidents each day. These incidents are recorded mainly by logging and computer security software. Centralized logging and event correlation software can be effective in automating the initial analysis of the voluminous data that is collected and in selecting the events of interest that require human review. To assure the quality of the data collected, organizations should establish logging standards and procedures that facilitate the collection of adequate information by logs and security software. This data should be reviewed regularly by the appropriate staff members.

Develop written guidelines for prioritizing incidents.

Prioritizing the handling of individual incidents is a critical decision point in the incident response process. Incidents should be prioritized based on the following:

- Criticality of the affected resources and data, such as whether a public Web server or a user workstation is affected; and
- Current and potential technical effect of the incident, such as root compromise or destruction of data.

Combining the criticality of the affected resources and the current and potential technical effect of the incident determines the impact of the incident to the organization. For example, data destruction on a user workstation might result in a minor loss of productivity; however, root compromise of a public Web server might result in a major loss of revenue, productivity, access to services, and reputation, as well as the release of sensitive data. The latter breach could result in the release of credit card numbers, Social Security numbers, and other forms of personally identifiable information.

Since incident handlers may be under great stress during incidents, it is important to make the prioritization process clear. Organizations should decide how the incident response team should react under various circumstances and then create a Service-Level Agreement (SLA) that documents the appropriate actions and maximum response times. This documentation is particularly valuable for organizations that outsource components of their incident response programs. Documenting the guidelines should facilitate faster and more consistent decision making.

Review the lessons learned from security incidents to improve the organization's security incident handling processes.

After a major incident has been handled, the organization should hold a meeting to review the lessons learned from the incident and the effectiveness of the incident handling process. Then it is possible to identify necessary improvements to existing security controls and practices. Meetings to review lessons learned should also be held periodically for lesser incidents. The information accumulated from all of the meetings to review the lessons learned should be used to identify systemic security weaknesses and deficiencies in policies and procedures. Follow-up reports generated for each resolved incident can be important not only for evidentiary purposes but also for reference in handling future incidents and in training new members of the incident response team. An incident database, with detailed information on each incident that occurs, can be another valuable source of information for incident handlers.

Seek to maintain situational awareness during large-scale incidents.

Organizations often are challenged to maintain situational awareness for handling of large-scale incidents because these incidents are very complex. Many people within the organization may play a role in the incident response, and the organization may need to communicate rapidly and efficiently with various external groups. Collecting, organizing, and analyzing all the pieces of information, so that the right decisions can be made and executed, are not easy tasks. The key to maintaining situational awareness is to prepare to handle large-scale incidents by:

- Establishing, documenting, maintaining, and exercising

on-hours and off-hours contact and notification mechanisms for various individuals and groups within the organization, such as the chief information officer (CIO), head of information security, IT support staff, and business continuity planning staff. Mechanisms are also needed for contacts outside the organization, such as US-CERT, incident response organizations, and counterparts at other organizations;

- Planning and documenting guidelines for the prioritization of incident response actions based on business impact;
- Preparing one or more individuals to act as security incident leads with responsibility for gathering information from the incident handlers and other parties, and distributing relevant information to the parties that need it; and
- Practicing the handling of large-scale incidents through exercises and simulations on a regular basis. Since these incidents happen rarely, incident response teams often lack experience in handling them effectively.

More Information

See Appendix J of SP 800-61 Revision 1 for information about federal incident reporting guidelines, including definitions and reporting time frames. The US-CERT Web page can be found at:

http://www.us-cert.gov/federal/reportingRequirements.html.

OMB directives and guidelines are available at:

http://www.whitehouse.gov/omb/.

NIST publications assist organizations in planning and implementing a comprehensive approach to information security. See NIST's Web page for information about NIST standards and guidelines that are referenced in the Computer Security Incident Handling Guide and other security-related publications, covering related topics, such as security planning, risk management procedures, security controls, intrusion detection systems, and firewalls. http://csrc.nist.gov/publications/index.html

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.