ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

COMPUTER SECURITY INCIDENTS: ASSESSING, MANAGING, AND CONTROLLING THE RISKS

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

Attacks on computers and networks have become more numerous and more severe in recent years. While preventing such attacks would be the ideal course of action for organizations, not all computer security incidents can be prevented. Every organization that depends upon computers and networks to carry out its mission should identify and assess the risks to its systems and to its information, and reduce those risks to an acceptable level. An important component of this risk management process is the assessment of the risks of security incidents and the identification of effective ways to deal with them. A well-defined incident response capability helps the organization detect incidents rapidly, minimize losses and destruction, identify weaknesses, and restore information technology operations speedily.

NIST Guide on Handling Security Incidents

NIST's Information Technology Laboratory recently issued Special Publication (SP) 800-61, *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology.* Written by Tim Grance, Karen Kent, and Brian Kim, NIST SP 800-61 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 new guide replaces NIST SP 800-3, *Establishing a Computer Security Incident Response Capability (CSIRC).*

The new incident handling guide contains useful information for computer security incident response teams (CSIRTs), system and network administrators, security staff, technical support staff, chief information officers (CIOs), and computer security program managers who are responsible for handling security incidents. Topics discussed include the need for and the organization of incident response teams, and how to manage the incident handling process. Specific recommendations are provided for handling five types of incidents: denial of service (DoS), malicious code, unauthorized access, inappropriate usage, and multiple component incidents.

Appendices include a consolidated list of recommendations that are discussed in the guide, incident response scenarios, and questions for use in incident response exercises. Also included in the appendices are suggested items of information to be collected about each incident, a glossary, an acronym list, lists of online resources and other references, frequently asked questions about incident response activities, and the steps to follow when handling a security incident.

This *ITL Bulletin* summarizes NIST SP 800-61, which is available at http://csrc.nist.gov/publications/nistpubs/index.html.

Planning and organizing an incident handling capability

Federal departments and agencies are specifically directed by the Federal Information Security Management Act (FISMA) of 2002 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 Federal

Continued on page 2

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 8901, Gaithersburg, MD 20899-8901, 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 October 2002

- *Security Patches and the CVE Vulnerability Naming Scheme: Tools to Address Computer System Vulnerabilities*, October 2002
- *Security for Telecommuting and Broadband Communications*, November 2002
- *Security of Public Web Servers*, December 2002
- *Security of Electronic Mail*, January 2003
- *Secure Interconnections for Information Technology Systems*, February 2003
- *Security for Wireless Networks and Devices*, March 2003
- *ASSET: Security Assessment Tool for Federal Agencies*, June 2003
- *Testing Intrusion Detection Systems*, July 2003
- *IT Security Metrics*, August 2003
- *Information Technology Security Awareness, Training, Education, and Certification*, October 2003
- *Network Security Testing,* November 2003
- *Security Considerations in the Information System Development Life Cycle*, December 2003

Computer Incident Response Center (FedCIRC) in the Department of Homeland Security, and for documenting corrective actions that have been taken and their impact. Further, 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).

The participation of many people within the organization is important in planning and implementing an incident response program, and in making the decisions that are key to a successful program. The organization should adopt an incident response policy which defines which events are considered incidents, establishes the organizational structure for incident response, defines roles and responsibilities, and lists the requirements for reporting incidents.

An incident response team with appropriate technical skills should be selected from the different team structures and staffing models that are discussed in the guide, and training should be provided to team members. The services that will be provided by the team should be decided. Procedures are needed to assess the impact of incidents, and effective methods of collecting, analyzing, and reporting data should be established. Careful planning and dedicated resources are essential to establishing and maintaining a successful incident handling capability that will enable the organization to respond quickly and effectively when incidents occur.

Who we are

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our website is http://www.itl.nist.gov/.

Using effective security methods for networks, systems, and applications to reduce the frequency of incidents

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. Risk assessments should be performed regularly and the identified risks reduced to an acceptable level. Threats to systems and information should be continuously monitored using intrusion detection systems and other methods. The incident response team should have access to tools, resources, and information such as contact lists, encryption software, network diagrams, and security patches. When the security of networks, systems, and applications is effectively protected and maintained, the incident response team can focus on handling serious problems. See Sections 3.1, 4.2, 5.2, 6.2, and 7.2 of the guide for specific recommendations for maintaining adequate security.

Interacting with other organizations

Clear procedures should be established to communicate when necessary with internal groups such as the human resources, public affairs, and legal departments, and with external organizations such as computer incident response teams and law enforcement officials. A list of such contacts should be developed and maintained. Guidelines are needed so that only the appropriate information is shared with the right parties. The inappropriate release of sensitive information could lead to greater disruption and financial loss than the incident itself by revealing information useful to the attacker or another would-be attacker.

Maintaining staff awareness of the importance of incident detection and analysis

Logging and computer security software should be checked for possible signs of incidents. Event correlation software and centralized logging can be of great value in performing an initial analysis of the voluminous data that is collected and in selecting the events that require human review. The effectiveness of the automated analysis process depends on the quality of the data that is collected. Organizations should establish standards and procedures to make certain that adequate information is collected by the logging and security software, and to assure that data collected and analyzed by the automated software is reviewed regularly by staff members.

Developing written guidelines for prioritizing incidents

Priorities for the handling of individual incidents should be established, based on the following considerations:

- The criticality of the affected resources (e.g., public web server, user workstation)
- The current and potential technical effect of the incident (e.g., root compromise, data destruction).

The business impact of the incident depends upon these considerations. For example, data destruction on a user workstation might result in a minor loss of productivity. 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 confidential data, such as credit card numbers or Social Security numbers.

Clear decisions about priorities and how to react in various circumstances will help the incident response team respond quicker and more effectively, thereby reducing the cost, duration, and overall business impact on the organization. The organization should develop a Service Level Agreement (SLA) to document the appropriate actions and maximum response times. This documentation is particularly valuable for organizations that outsource components of their incident response programs.

Applying the lessons learned from incidents

After a major incident has been handled, the organization should hold a meeting to review how effective the incident handling process was and to identify needed improvements to existing security controls and practices. Meetings to go over lessons learned should also be held periodically for lesser incidents. The information accumulated from all of these review meetings should be used to identify systemic security weaknesses and deficiencies in policies and procedures. The follow-up reports generated for each resolved incident can be valuable for evidentiary purposes, for reference in handling future incidents, and in training new incident response team members. An incident database, with detailed information on each incident that occurs, can be another useful source of information for incident handlers.

Maintaining situational awareness during large-scale incidents

Communications within the organization and with external groups can be challenging and complex when large-scale incidents are handled. Many people within the organization may play a role in incident response, and the organization may need to communicate rapidly and efficiently with various external groups. Many pieces of information must be collected, organized, and analyzed to enable the right decisions to be made and executed. Situational awareness in the organization can be maintained when handling 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 (e.g., chief information officer [CIO], head of information security, IT support, business continuity planning) and outside the organization (e.g., incident response organizations, 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 lead officials who are responsible for gathering information from the incident handlers and other parties, and distributing relevant information to the parties that need it.
- Practicing the handling of large-scale incidents through exercises and simulations on a regular basis. Such incidents happen rarely, so incident response teams often lack experience in handling them effectively.

Handling specific types of incidents

NIST SP 800-61 specifies recommended procedures for preventing and dealing with the following kinds of incidents:

- **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 infects a host
- **Unauthorized Access—**a person gains logical or physical access without permission to a network, system, application, data, or other resource
- **Inappropriate Usage—**a person violates acceptable computing use 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.

Check the guide for detailed recommendations and advice to prevent and reduce the damage that might be caused by each of these kinds of incidents.

More Information

For a list of references, online tools, and resources on incident response activities, consult Appendices F and G of NIST SP 800-61.

The following Special Publications (SPs) provide help to organizations in planning, developing, operating, and maintaining incident response programs. These publications are available in electronic format from the NIST Computer Security Resource Center at http://csrc.nist.gov/publications.

NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*, discusses developing and updating security plans.

NIST SP 800-28, *Guidelines on Active Content and Mobile Code*, gives advice on the use of active content (e.g., java applets, macros, etc.), identifies the risks, and suggests strategies for managing these risks.

NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, discusses the risk-based approach to security and provides guidance on conducting risk assessments.

NIST SP 800-31, *Intrusion Detection Systems (IDSs),* and NIST SP 800-41, *Guidelines on Firewalls and Firewall Policy*, provide information on using and deploying IDSs and firewalls.

NIST SP 800-35, *Guide to Information Technology Security Services*, covers evaluating, selecting, and managing security services throughout the life cycle.

NIST SP 800-40, *Procedures for Handling Security Patches*, provides guidance on suggested polices and methods to systematically and effectively implement an organizational patch management strategy.

NIST SP 800-42, *Guidelines on Network Security Testing*, describes available security testing techniques, their strengths and weaknesses, and the recommended frequencies for testing as well as strategies for deploying network security testing.

ITL Bulletins Via E-Mail
We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message from your business e-mail account to listproc@nist.gov with the message **subscribe itl-bulletin**, and your name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message **HELP**. To have the bulletin sent to an e-mail address other than the From address, contact the ITL editor at 301-975-2832 or elizabeth.lennon@nist.gov.

NIST SP 800-44, *Guidelines on Securing Public Web Servers*, and NIST SP 800-45, *Guidelines on Electronic Mail Security*, assist organizations in installing, configuring, and maintaining secure public web servers and e-mail servers.

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, provides recommended security controls based on system impact level (available in draft at http://csrc.nist.gov/publications/drafts.html).

The following organizations (and others listed in Appendix G of the guide) provide useful information on incident handling:

Federal Computer Incident Response Center (FedCIRC), the federal government's incident response activity
http://www.fedcirc.gov

CERT® Coordination Center (CERT®/CC), nongovernmental incident response activity located at Carnegie Mellon University
http://www.cert.org

Information Analysis Infrastructure Protection (IAIP) in the Department of Homeland Security (DHS)
http://www.nipc.gov

Center for Education and Research in Information Assurance and Security (CERIAS®) at Purdue University
https://cirdb.cerias.purdue.edu

SANS Institute Reading Room
http://www.sans.org/rr

National Institute of Justice (NIJ) Electronic Crime Program
http://www.ojp.usdoj.gov/nij/sciencetech/ecrime.htm

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.

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900

Official Business
Penalty for Private Use $300

Address Service Requested

PRSRT STD
POSTAGE & FEES PAID
NIST
PERMIT NUMBER G195