ITL BULLETIN FOR SEPTEMBER 2012

REVISED GUIDE HELPS ORGANIZATIONS HANDLE SECURITY-RELATED INCIDENTS

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

To protect their information and information systems, organizations must deal with ever-changing cybersecurity attacks and threats that are occurring more frequently, and that often result in damage and disruption to systems. The organization's response to computer security incidents is an important component of its information technology (IT) security programs.

Security incidents are violations or threats of violation of the organization's computer security policies, acceptable use policies, or standard computer security practices. While preventive activities based on the results of risk assessments can lower the number of incidents, not all incidents can be prevented. Organizations need an incident response capability to enable them to detect incidents quickly, minimize loss and destruction, mitigate the system weaknesses that were exploited, and restore IT services.

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) recently revised its guidelines for computer security incident handling to address the new and changing threats and attacks that are occurring. The new publication, NIST Special Publication (SP) 800-61 Revision 2, *Computer Security Incident Handling Guide*, highlights the importance of analyzing incident-related data and determining the appropriate response to each incident. The guidelines can be broadly applied a wide variety of hardware platforms, operating systems, protocols, and applications.

NIST Special Publication (SP) 800-61 Revision 2, *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology*

This publication assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively. It emphasizes the importance of understanding the threats, identifying current attacks in their early stages in order to prevent subsequent damage and disruption, and sharing information to help other organizations identify similar threats and attacks. SP 800-61 Revision 2 was written by Paul Cichonski of NIST, Tom Millar of the United States Computer Emergency Readiness Team (US-CERT), Tim Grance of NIST, and Karen Scarfone of Scarfone Cybersecurity. Topics covered in the publication include:

- How to organize a computer security incident response capability; why an incident response capability is needed; examples of incident response team structures; how to involve other groups within an organization to support the incident handling teams;
- How to handle an incident; the basic incident handling steps; techniques for more effective incident handling, particularly incident detection and analysis; and
- How to manage and coordinate incident response and information sharing with other organizations, including law enforcement and the media.

The guidelines for establishing, maintaining, and improving incident response capabilities that are discussed in SP 800-61 Revision 2 are supplemented with extensive information and additional details in appendices to the publication, including:

- Incident response scenarios and questions for use in staff discussions to build incident response skills and identify potential issues in incident response processes;
- Lists of suggested incident-related data elements to be collected when an incident is reported and when incident handlers respond;
- A glossary of terms used in the publication;
- A list of acronyms;
- Resources that organizations may find useful when planning and performing incident responses;
- Frequently asked questions about incident response;
- The major steps to follow when handling a computer security incident-related crisis; and
- A change log listing significant changes in the guidelines since the previous revision was issued.

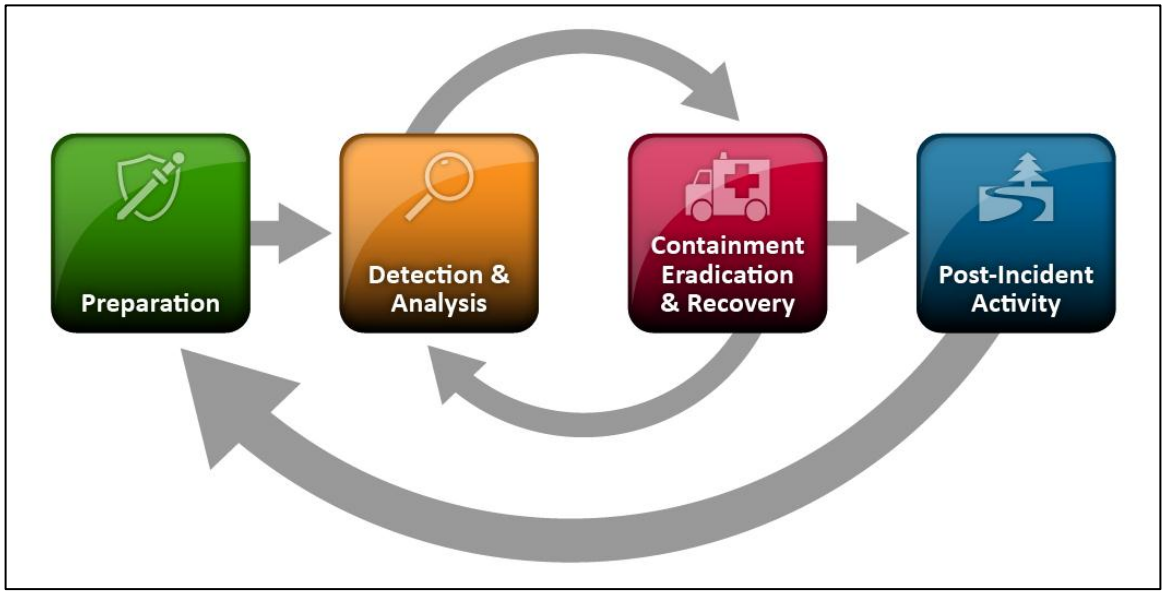
NIST SP 800-61 Revision 2 is available on the NIST Computer Security Resource Center (CSRC) web page:
http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf.

Organizing a Computer Security Incident Response Capability

Organizing a computer security incident response starts with establishing an organization-specific definition of the term “incident,” and deciding what services the incident response team should provide. Other issues include determining which team structures and models can provide the identified services, and then selecting and implementing one or more incident response teams. The organization’s incident response plan, policies, and procedures support: establishing a team; enabling incident response to be performed effectively, efficiently, and consistently; and empowering the team to do what needs to be done. The plan, policies, and procedures should state the team’s interactions with other teams within the organization as well as with outside parties, such as law enforcement, the media, and other incident response organizations.

Handling an Incident

The phases of the incident response process are preparation, detection and analysis, containment, eradication and recovery, and post-incident activity. The preparation phase of the process involves establishing and training an incident response team, and acquiring the necessary tools and resources. During preparation, the organization applies security controls that are selected based on the results of risk assessments in order to limit the number of incidents that will occur. Since risks are persistent and constantly changing, incidents can occur despite the application of controls. Detection of security breaches is necessary to alert the organization whenever incidents occur. Depending upon the severity of the incident, the organization can mitigate the impact of the incident by containing it and ultimately recovering from it. During this phase, incident response activity often goes back to the detection and analysis phase to see if additional hosts have been affected by the security incident. 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.

Coordination and Information Sharing

The persistence and nature of contemporary threats and attacks make it more important than ever for organizations to work together during incident response. Organizations should ensure that they effectively coordinate portions of their incident response activities with appropriate partners. Coordinating and sharing information with partner organizations can strengthen the organization's ability to respond more quickly and efficiently to IT incidents.

An important part of incident response coordination is information sharing. When different organizations share threat, attack, and vulnerability information with each other, each organization's knowledge benefits the other. Often the same threats and attacks affect many organizations simultaneously. Small organizations, without in-house resources to fully analyze incidents, can benefit from the technical capabilities of a trusted information-sharing network.

NIST Recommendations for Improving Security Incident Response Activities

NIST recommends that organizations implement the following practices and procedures to improve the efficiency and effectiveness of their security incident response activities:

• Create, support, and operate a formal incident response capability. Federal agencies are required to report incidents to the United States Computer Emergency Readiness Team (US-CERT) office within the Department of Homeland Security (DHS), in accordance with the Federal Information Security Management Act of 2002.

The Federal Information Security Management Act (FISMA) requires federal agencies to establish incident response capabilities. Each federal civilian agency must designate a primary and secondary point of contact (POC) with US-CERT and report all incidents consistent with the agency's incident response policy. Each agency is responsible for determining how to fulfill these requirements.

The steps in establishing an incident response capability include:

· Creating an incident response policy and plan;
· Developing procedures for performing incident handling and reporting;
· Setting guidelines for communicating with outside parties regarding incidents;
· Selecting a team structure and staffing model;
· Establishing relationships and lines of communication between the incident response team and other groups, both internal and external to the organization;
· Determining what services the incident response team should provide; and
· Staffing and training the incident response team.

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

Preventing problems is often less costly and more effective than reacting to them after they occur. Incident prevention is an important component of the organization's security planning, implementation, and management, and a requirement for an effective incident response capability. If security controls are inadequate and weak, many security-related incidents may occur. This could overwhelm the organization's resources and capacity for response, and could

result in delayed or incomplete recovery, more extensive damage, and longer periods when service and data are not available. Incident handling can be performed more effectively if organizations support their incident response capability with adequate resources to actively maintain the security of networks, systems, and applications. This includes training IT staff on complying with the organization's security standards and making users aware of policies and procedures regarding the appropriate use of networks, systems, and applications.

• Document organizational guidelines for interactions with other organizations regarding incidents.

During the incident handling process, the organization will need to communicate with outside parties, such as other incident response teams, law enforcement, the media, vendors, and those affected by the incident. Because these communications often need to take place quickly, organizations should determine communication guidelines in advance so that only the appropriate information is shared with the right parties.

• Be generally prepared to handle any incident but focus on being prepared to handle incidents that use common attack vectors.

Incidents can occur in countless ways, so it is not feasible to develop step-by-step instructions for handling every incident. While SP 800-61 Revision 2 defines several types of incidents, based on common attack vectors, these categories may not provide definitive classification for all incidents, and should be used as a basis for defining more specific handling procedures. Different types of incidents call for different response strategies. The attack vectors are:

· **External/Removable Media:** An attack executed from removable media, such as a flash drive or disk, or a peripheral device;
· **Attrition:** An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services;
· **Web:** An attack executed from a website or web-based application;
· **Email:** An attack executed via an email message or attachment;
· **Improper Usage:** Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories;
· **Loss or Theft of Equipment:** The loss or theft of a computing device or media used by the organization, such as a laptop or smart phone; and
· **Other:** An attack that does not fit into any of the other categories.

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

An organization's logging and computer security software may record countless signs of incidents occurring each day. Automated techniques are needed to perform an initial analysis

of the data and to select the events of interest for human review. Event correlation software can be very useful in automating the analysis process. However, the effectiveness of the process depends on the quality of the data that is analyzed. Organizations should establish logging standards and procedures to ensure that adequate information is collected by logs and security software, and that the data is reviewed regularly.

• Create written guidelines for prioritizing incidents.

Prioritizing the handling of individual incidents is a critical decision point in the incident response process. Effective information sharing can help an organization identify situations that are of greater severity and that demand immediate attention. Incidents should be prioritized based on the relevant factors including: the functional impact of the incident, such as current and likely future negative impact to business functions; the impact of the incident on the confidentiality, integrity, and availability of the organization's information; and the organization's ability to recover from the incident, such as the time and types of resources that must be spent on recovering from the incident.

• Use the lessons learned from the incident response process to improve the handling of future incidents.

After a major incident has been handled, the organization should hold a meeting to discuss lessons learned, to review the effectiveness of the incident handling process, and to identify necessary improvements to existing security controls and practices. Meetings discussing lessons learned can also be held periodically for lesser incidents, as time and resources permit. The information accumulated from all lessons learned meetings should be used to identify and correct systemic 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 team members.

For More Information

The following NIST publications provide guidance and advice on activities that support computer security incident handling processes:

NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*
NIST SP 800-83, *Guide to Malware Incident Prevention and Handling* (This publication, which is being updated, will be issued as *Guide to Malware Incident Prevention and Handling for Desktops and Laptops.)*
NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*
NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*

NIST SP 800-92, *Guide to Computer Security Log Management*
NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*
NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*
NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*

For information about NIST standards and guidelines, and related publications, see the NIST web page: http://csrc.nist.gov/publications/index.html .

For information about NIST's cybersecurity programs, see the NIST web page: http://csrc.nist.gov.

ITL Bulletin Publisher:
Elizabeth Lennon, Writer/Editor
Information Technology Laboratory
National Institute of Standards and Technology
Email: elizabeth.lennon@nist.gov

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.