CSIRT
2362 Kanegis Dr
Waldorf, MD 20603

Tel: 1-301-275-4433 - USA 24x7

Incident Response: Martinez@csirt.org

Text Message: Text@csirt.org

Implementing an Incident Response Team (IRT)

1.0 Questions about this Document

This document examines the basic questions that must be addressed, when implementing an Incident Response Team (IRT), within an organization. It does not attempt to undertake an in-depth analysis of the requirements of an IRT, but provides a basic outline for such a team's organization and functions. This document can be used to better understand the duties and responsibilities of an IRT, and some of the pitfalls to avoid when creating one.

1.1 Copyright

2.0 Overview

The ability to react quickly to security incidents, when they occur, is the key component and most essential part of an overall security plan. An Incident Response Team's ability to operate effectively will depend on its ability to provide timely information to its clients regarding the electronic data environment it is commissioned to protect.

2.1 Definition of an Incident: An event which changes the security posture of an organization or circumvents security polices developed to prevent financial loss and/or the destruction, theft, or compromise of proprietary information. Also, an event investigated by an organization due to unusual activity, that cannot be explained as a consequence of normal operations.

2.2 Defining an Incident to the Constituency

Security Incidents must be clearly defined to the team's constituency, both management and the user community. The team

should publish flyers and documents to inform the users of current security threats as well as to reiterate the types of incidents that must be reported to the team. Providing such information to the user, is quite important, as incidents may otherwise go unreported due to lack of understanding. An internal website with general information about the IRT, including its mission, functions, and responsibilities, including contact data, is a must. However, procedures and polices of the team should not be published externally. Third parties, including hackers, may use such information to map and study an agency's weaknesses.

3.0 Government Agencies

Each agency should include a section within its overall security plan dedicated strictly to handling computer security incidents. It will define a means to detect, report, and investigate security incidents affecting that agency. However, cooperation and sharing information with other agencies is a critical component in the overall success of an IRT.

3.1 The planning stage

Categorization and prioritization of all information resources must be done at the very outset. Information from critical systems will receive a more direct and focused response as compared, for example, to information stored for future month's office supplies. For critical resources, an organization requires the ability to react to and recover from security incidents as they arise, with a swift, coordinated, and effective response, which will minimize the cost and damage to the organizational infrastructure as well as to its image as perceived by the user community.

Some possible classifications for security incidents are:

- Virus Attacks (Unable to clean, rename, or delete)
- Denial of Service Attack(s)
- IDS alert notification(s) (false positives possible)
- Automated scanning tools and probes
- Internal threats (espionage)
- Unauthorized accesses to information systems

3.2 Responsibilities

Organizations must share in the responsibility of coordinating their response efforts with other similar institutions. Gathering intelligence information from all sources is a critical part of information infrastructure protection. Networking in a trusted environment and sharing incident information and detection and response techniques can play an important role in identifying and correcting weaknesses. Without information sharing, government agencies such as US-CERT and law enforcement agencies are handicapped in their effort to alert other agencies to potential and/or actual threats directed at the critical information infrastructure of the United States.

3.3 Management Support

Effective incident response in any organization must begin with management. Management is responsible for providing the support, tools, personnel, and financial backing needed to ensure the successful implementation of an IRT. An IRT must be perceived well by all concerned. Security awareness training and briefings to senior management are some of the key components to a successful deployment of an IRT.

Sources of more information for building a Computer Security Incident Response Team (CSIRT) include:

- http://www.cert.org/CSIRTs/ CERT Coordination Center
- http://www.cert.org/training/2002/creating_CSIRT.html Creating a Computer Security Incident Response Team

- http://csrc.nist.gov/publications/nistpubs/800-3/800-3.pdf Establishing a Computer Security Incident Response Capability (CSIRC)

4.0 Mission Statement

The Team must have a Mission Statement that clearly states the constituency the team will serve and the authority or directive under which the team operates. The Mission Statement must have the explicit, written approval of management.

5.0 Placement of the Team

Placement in the management structure of an organization is also a factor in the success of an Incident Response Team. Conflicts of interest can and will occasionally arise due to political considerations and differing priorities within the structure of the organization. Since the Team may, due to technical expertise and knowledge requirements, comprise individuals from many departments within the organization, the Team must remain as flexible and as neutral as is possible. The ability to investigate security incidents thoroughly and resolve them effectively will depend on the resources available to the Team. The Team should not fall under the direct control of the security department, but should be able to act as an independent body with the ability to investigate security incidents free of departmental resource constraints. To this end, the resources available to the Team should be clearly specified in the team's charter.

6.0 Availability of the Team

The availability of the team is paramount. To maximize the full potential of the team, members must be available 24x7. Attacks can come at any hour. Intrusion Detection Systems (IDS) network and host-based, are playing a more critical role in identifying attacks and unusual activity, and alerts from such systems are generated at all hours of the day. A 24x7 incident response team allows an organization to respond to alerts generated by automated systems at any time. Monitoring systems and reviewing security alert information submitted by vendors is an important part of an incident response team's proactive duty. IDS systems by themselves do not provide a complete solution to identifying and responding to incidents; a security plan is needed to ensure overall protection that would include an incident response mechanism.

7.0 Clearance of Team Members

Due to possible sensitivity of materials, related to incidents, the team may come into contact with, all team members should pass a background check or a National Agency Check (NAC).

8.0 Developing Procedures

An incident response team must develop procedures to respond to particular types of incidents. Each type of incident needs to be clearly defined; this will enable members to react quickly and effectively. Procedures must detail the steps to be taken by team members when alerted of an incident of a particular type. Included within the procedures must be clearly defined criteria regarding investigative goals to be achieved before an incident can be closed. The team should also list and post contact information of key personnel and management to notify.

9.0 Outside Communications

The team may, at times, need to contact other organizations to assist in an investigation. The organization must develop a policy that clearly describes its position on the disclosure of incident information to the user community as well as to outside organizations such as CERT, US-CERT, and commercial incident response teams. Organizations may designate an individual (job function) to coordinate the exchange of information. All team member(s) must sign a non-disclosure form, to protect the interest of all parties concerned.

Contact information for security teams around the world:

- http://www.auscert.org.au/Information/Contact/irt.html Australian Computer Emergency Response Team
- http://www.first.org/team-info/ FIRST (Forum of Incident Response and Security Teams)

10.0 Tracking Incidents

Tracking of security incidents can become a full-time job. Incidents may remain open from a few hours to a few months, or even longer in some cases. The incident (case) record must contain all communications in connection with the incident from the time opened to the time of closure.

The manager or coordinator of the IRT must provide management reports on incidents investigated by the team. The team manager or coordinator must be held responsible for the closure of each incident. Incidents should be presented to management in the form of a formal report detailing steps taken, outcome of the incident, and lessons learned. Major incidents affecting the organizational infrastructure or its ability to perform its mission must be overseen and coordinated by senior management. The team manager or coordinator should give all formal briefings.

11.0 Evidence Collection

Depending on the type of incident, careful consideration should be given to the collection of any data that may be relevant to the incident. The team should develop procedures that clearly state the types of evidence to collect when an incident occurs. The types of evidence collected during an investigation will vary depending of the type of incident being investigated. team members should receive professional training in the protection of evidence (files, system logs, and backup tapes) in case such evidence needs to be used in a court of law. This training, while discussing general rules of evidence handling, should emphasize what *not* to do; i.e., what aspects of investigation and collection to leave to teams or agencies with specialized forensic training and experience as well as, in some instances, legal investigative authority.

11.1 Data mining

All organizations must address the data collection of raw data within their organization. This source of valuable information is widely overlooked. Data mining tools should be used to collect raw information from a variety of systems and telecommunication devices (switches, routers, firewalls, and gateways) across their agency. The correlation of raw data from different systems will enable the agency to identify different types and trends of attack tools used by hackers for reconnaissance purposes. These and other proactive activities of a team will complement the security posture of any organization.

12.0 Reporting to US-CERT

Government agencies are also required to report security incidents to US-CERT. US-CERT compiles incident reports from many government agencies to provide incident statistics of types of incidents across the Federal government. US-CERT also provides assistance to Federal agencies in the event of an intrusion. However, different agencies may classify a given incident differently, and because of this, agencies may report the same or similar incidents as various types and in various numbers. As of this date there is not yet a definite consensus amongst the security community as to what a security incident is or how they should be classified.

13.0 Performance Goals and Accomplishments

A key area overlooked by most teams is performance goals and how accomplishments of the team are measured against them.

The establishment of performance goals by the team and the endorsement of these goals by management will hopefully prevent the team from becoming a clearinghouse for unwanted or un-categorized security projects. Also, only by clearly defining team goals will management will be able to ascertain how effectively the team is performing. The team must also perform internal audits to correct any problems discovered. Identifying performance goals of the team will aid in justification of current and future resources.

14.0 Where to Find Help

Networking with other government incident response teams is a great way to start learning standard practices of incident response and procedure development. Learning from other experienced teams who have already experienced some of the pitfalls is the best way to avoid repeating mistakes; there is no point in reinventing the wheel. The sharing of audit findings, from GAO and in-house audits, is also a source of a great wealth of information, especially when shared between different agencies.

Here are some URLs for contacting other incident response teams within the government:

- http://www.US-CERT.gov/ US-CERT (Federal Computer Incident Response Center)
- http://www.ciac.org/ciac/ U.S. DOE-CIAC (Computer Incident Advisory Capability)
- http://www-nasirc.nasa.gov/ National Aeronautics and Space Administration
- http://www.house.gov/ushcert/ **HOUSECIRT** (United States House of Representatives Computer Incident Response Team)

15.0 Conclusion

Establishing an Incident Response Team within a federal agency can be an overwhelming task. There are many different publications within the Government that can provide guidelines on the establishment of an IRT. When the time arrives for your team to be audited by the GAO (General Accounting Office), they may reference many different publications in testing the effectiveness of your team. Listed below are just some of the publications you will need to become familiar with. If you fail to understand how an incident response team operates, or its interaction within the Federal Government, your team may fail miserably. On the other hand, if you understand how the Government expects an Incident Response Team to operate, and what rules and documents are used in measuring its compliance and effectiveness, you stand a much better chance of emerging from such a test with your team not only in one piece, but held in high regard.

16.0 Supporting documentation

CIRCULAR NO. A-130 Circular No. A-130 provides uniform government-wide information resources management policies as required by the Paperwork Reduction Act of 1980, as amended by the Paperwork Reduction Act of 1995, 44 U.S.C

Government Information Security Reform Act This document details the on the FY 2001 Defense Authorization Act (P.L. 106-398) including Title X, subtitle G, "Government Information Security Reform." As found in existing policy, all agency programs will include procedures for detecting, reporting, and responding to security incidents, including notifying and consulting with law enforcement officials, other offices and authorities, and the General Services Administration's Federal Computer Incident Response Capability (FedCIRC).

Agency Interaction with GSA's Federal Computer Incident Response Capability (FedCIRC) The attachment to this memo describes the process that agencies should follow for appropriate coordination and interaction with GSA's Federal Computer Security Incident Response Capability (FedCIRC), to ensure that: 1) externally generated security incidents are reported to FedCIRC; 2) alerts and warnings from FedCIRC are received by responsible individuals in the agencies; and 3)

when necessary, positive acknowledgment of receipt and reporting of corrective actions is provided to FedCIRC.

An Introduction to Computer Security: The NIST Handbook Special Publication 800-12. Chapter 12 COMPUTER SECURITY INCIDENT HANDLING. An incident handling capability also assists an organization in preventing (or at least minimizing) damage from future incidents. Incidents can be studied internally to gain a better understanding of the organization's threats and vulnerabilities so more effective safeguards can be implemented.