Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Building an Incident Response Program To Suit Your Business

The purpose of this paper is to outline the key concepts of an Incident Response Program (IRP). Although every organization is unique, there are basics components that should be included to mitigate disaster. This paper is in no way meant to be a comprehensive program for an IRP and should only be viewed as a starting point. For an IRP to be successful, the maintenance of the Program is an on-going process that must be kept current and reflect organizational / infrastructure changes and newly discovered vulnerabilities...

Copyright SANS Institute
Author Retains Full Rights

AD

Beating the IPS?

GIAC Security Essentials (v 1.2e)
July 3, 2001

Building an Incident Response Program To Suit Your Business

By: Tia R. Osborne

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Table Of Contents

Building an Incident Response Program To Suit Your Business..... 3
What is an Incident Response Program? 3
Why is an Incident Response Program necessary? 3
Who in the organization should be responsible for handling incidents?..... 3
How much does an Incident Response Program cost?..... 4
What are the components of an Incident Response Program?..... 5
Reporting/Discovery..... 5
Response 6
Investigation..... 7
Recovery 7
Follow-up..... 7
List of References: 8
Practical Questions..... **Error! Bookmark not defined.**

© SANS Institute 2001, Author retains full rights

Building an Incident Response Program To Suit Your Business

What is an Incident Response Program?

A security incident refers to an adverse event in an information system, and/or network, or the threat of the occurrence of such an event. Incidents can include but are not limited to unauthorized access, malicious code, network probes and denial of service attacks (1). Regardless of the criticality of the incident, it is essential that all steps outlined in this program are followed and are.

The purpose of this paper is to outline the key concepts of an Incident Response Program (IRP). Although every organization is unique, there are basics components that should be included to mitigate disaster. This paper is in no way meant to be a comprehensive program for an IRP and should only be viewed as a starting point. For an IRP to be successful, the maintenance of the Program is an on-going process that must be kept current and reflect organizational / infrastructure changes and newly discovered vulnerabilities as they occur. In addition, an IRP should be a key component to a well-rounded information security program that includes Policies and Procedures, a Compliance Monitoring Program and an Intrusion Detection System.

Why is an Incident Response Program necessary?

Due to the nature and amount of business being done through the Internet, minimizing security vulnerabilities and responding to security incidents in an efficient and thorough manner can become critical to business continuity. However, the scale of a response is dictated by the nature of each individual organization. An organization that does little e-commerce can be more apt to disconnect their network at a moment's notice without much harm to it's revenue, yet an organization whose mainstay is e-commerce may want to investigate more resources into developing an in-depth IRP.

Who in the organization should be responsible for handling incidents?

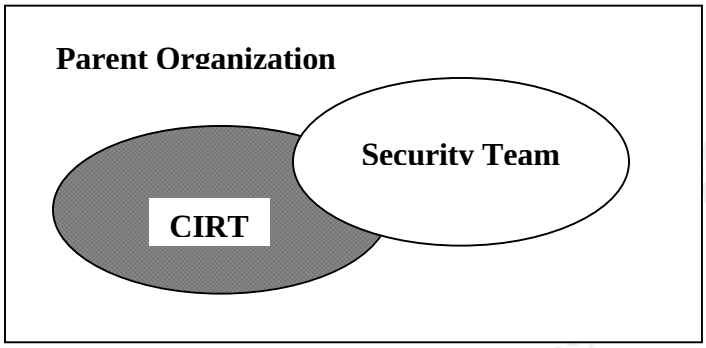
An organization should develop a group of individuals that are responsible for handling incidents, a Computer Incident Response Team. Computer Incident Response Team (CIRT) Members who are identified in the organization should serve as champions of the IRP (2). Depending on the size of the organization, there may be only a small number of people acting as informal CIRT members, whereas in a larger e-commerce organization, the CIRT will be larger and more formal. CIRT Members should be responsible for the following areas:

- development and preservation of the program and the document,
- defining and classifying incidents,
- determining the tools and technology utilized in intrusion detection,
- determining if incident should be investigated and the scope of such an investigation (i.e. law enforcement agencies, forensic work),
- securing the network,
- conducting follow-up reviews,

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- and promoting awareness throughout the organization (2).

Moreover, the CIRT members must ensure the program reflects the business strategy of the organization as well as the information security group and ultimately have the support of executive management. An IRP should be developed in accordance with an organization's Information Security Policies and Procedures.



CIRT within an organization (2)

An IRP should be maintained in both an electronic format and a hard copy. Upon significant revisions, both should be updated appropriately. In order to facilitate this process, an email distribution list should be established to ensure all CIRT members are made aware of any notifications, updates or revisions as well as relevant communications.

How much does an Incident Response Program cost?

An Incident Response Program is at times difficult to gain the respect and commitment of upper management due to the cost as well as the fact that an IRP or parts of an IRP, may infrequently or never be used. The budget numbers supplied below by Gartner (5) are extensive as is the IRP that is based off of those numbers. In addition, these projections would only be maximized the most by a large organization and / or an organization that has depends largely on its e-commerce.

- 2 dedicated CIRT people reporting to the chief information security officer
- @251,000 per-person start-up capital expenditure
    - Hardware - $144,000
    - Software - $80,000
    - Education - $27,000 first year training, $27,000 every year after
- Stand-Alone CIRT command central reporting center
- Telecommunications – 24 lines, 8 each voice, data, fax
- External services – investigations and forensics - $100,000/year
- During the incident, need support from:
    - Network engineering (1 person per-platform)
    - Legal (1 person)
    - Human Resources (1 person)
    - PR (1 person)

It is important to keep in mind these figures to signify the cost of such a program, and to more importantly weigh in the cost to one's organization by such means of reputation and legal in ***not*** having such a program.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

What are the components of an Incident Response Program?

The following points summarizes the aspects of reporting, discovering, responding, investigation, recovery and follow-up of an incident within an organization:

Reporting/Discovery

- **Monitor Vulnerability Advisories Daily**

An integral part of an IRP is the ability of an organization to ensure its information systems are appropriately patched and updated. The Internet provides a valuable resource that allows organizations to monitor the release of patches and upgrades from vendors. The following table identifies such resources:

Organization	Website
CERT® Advisories	http://www.cert.org/advisories/
Security Focus	http://www.securityfocus.com/
Sun Solaris	http://sunsolve.sun.com/security
Microsoft	http://www.microsoft.com/technet/security/current.asp
Cisco	http://www.cisco.com/warp/public/770/
Netscape	http://home.netscape.com/security/notes/index.html
Checkpoint	http://phoneboy.com/fw1/

- **Monitoring Logs**
  Logs should be monitored in order for incidents to be identified. Monitoring could be by accomplished through manual means and/or an Intrusion Detection System.

- **Automatic Notification**
  Identified CIRT Members should be altered to high-risk security incidents through means of pager, voicemail and/or email.

- **Incident Response Tracking Database**
  A database should be developed to track all reported security incidents. This may facilitate the organization in warding off future incidents.

- **Classification / Identification of an Incident**

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

All reported incidents should be classified as a high/medium/low risk to facilitate the appropriate actions to take. Each organization will have its own risk rating for particular incidents. The following table provides a small example of the incident classifications:

Criticality	Definition	Examples
High	Incidents that *have a monumental* impact on the organization's business or service to customers.	• Malicious code attacks, including Trojan horse programs and virus infestations
		• Unauthorized system access
Medium	Incidents that *has a significant* or *has the potential to have a monumental* impact on the organization's business or service to customers.	• Password cracking attempts
		• Password does not allow access to system, apparent change of password without user knowledge has occurred
Low	Incidents that *has the potential to have a significant or monumental* impact on the organization's business or service to customers.	• Probes and network mapping
		• Denial of access to the system due to unexpected lockout

Response

Once an Incident has been reported, the appropriate CIRT member should be notified. CIRT member(s) will be responsible for performing the initial investigation to determine if an incident has occurred. The following checklist identifies steps that can be used to facilitate in classifying the incident, if one in fact has occurred (6):

- Log files
- Privileged programs
- System file tampering
- Sniffer Programs
- Unauthorized services
- Password file changes
- Check system and network configurations
- Look for unusual files
- Examine other hosts.

In addition, there are several "quick solutions" that can facilitate stopping an intrusion from propagating further. These solutions include blocking the IP from which the attack is being generated, disabling the affected userid, remove/block the system from the network and shutting the system down. Due to the multitude of intrusions that can take place and the risk involvement, it is imperative individual organizations decide on which method of response to

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

follow. Moreover, it must be realized that decisions made have the potential to affect other corporate systems and people as well as customers service.

Investigation

Depending on the level of intrusion and corresponding criticality, an organization may decide to perform a forensic investigation. A forensic investigation will allow the affected organization to gain a better understanding of the intrusion and the attacker. Computer forensic activity requires a comprehensive understanding of systems and networks due to the inherent complexity and volatility. A forensic expert will extract the needed information from the compromised system(s) without altering the original data. In order to interpret the degree to which malicious activity has occurred and to understand the extent of the incurred damage, the forensic investigation is dependent upon the preservation of the information. Again, depending upon the size of the organization, it may be more fruitful to outsource forensic involvement to reduce the cost of in house training and continuing education.

If an organization decides to participate in forensic investigation and it has been completed, there may be a great deal of information that will result from such investigation. These include security vulnerabilities that exist in the organization's systems, any changes to be made to the systems and/or applications, identification of the source(s) of the attack and methods of information disclosure, including acts of espionage.

Recovery

A main purpose of an Incident Response Program is to ensure an efficient recovery through the eradication of security vulnerabilities and the reinstatement of repaired systems. Recovery includes ensuring the attacker's points of penetration and any associated vulnerabilities have been eliminated and all systems have been restored. Moreover, depending on the type of incident, various methods of recovery exist. Identified CIRT members or owners should work in conjunction with the Business Continuity Planning team to ensure efforts made by each team can be leveraged (i.e. if the IRP states additional servers will be used while the recovery period is in effect, the BCP should be involved to ensure such servers exist).

Follow-up

It is imperative that an organization learns from incidents that occur. This will allow the organization to facilitate in reducing the likelihood of an incident from reoccurring. Incidents should be tracked and reported appropriately. In addition, an awareness and training program should be developed to ensure all members of an organization are aware of what constitutes a security incident and who the appropriate personnel are to handle the situation. Depending upon the nature of the organization's Incident Response Program, it may be necessary to have meetings involving CIRT members and executive management to bring everyone up to date on the latest risk and to ensure full support from executive management. In addition the results from such a meeting as well as the information surrounding the incidents can be organized in an Incident Response Database for future reference.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

List of References:

1 Northcutt, Stephen. Computer Security Incident Handling Step By Step. The Sans Institute, 1998.

2 Cert Organization. Preparing For and Responding to Security Incidents. 19 March 2001. http://www.cert.org/present/cert-overview-trends/tsld223.htm. (5 July 2001).

3 Malisow, Bill. Moments Notice: The Immediate Steps of Incident Handling. 7 July 2000. http://www.securityfocus.com. (5 July 2001).

4 CERT Coordination Center Software Engineering Institute. Incident and Vulnerability Trends. 17 August 2000. http://www.cert.org/present/cert-overview-trends/sld015.htm. (5 July 2001).

5 Spernow, William. Developing a Cyber Emergency Response Team. Gartner, 2000. 18.

6 Amoroso, Edward. Intrusion Detection. Sparta: Intrusion.Net Books, 1999. 200.

© SANS Institute 2001, Author retains full rights

Last Updated: May 23rd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced