Global Information Assurance Certification Paper

Chris Thompson
Version 1.2f

Incident Response and Creating the CSIRT in Corporate America

Introduction

There are many challenges faced by the brave few who have tried to implement a formal incident response mechanism within a corporation. They usually face a number of barriers that eventually wear down even the most stalwart of advocates. These challenges usually come in the form of politics.

The purpose of this document is to discuss why these challenges may exist and suggest a way to successfully implement a formal incident response organization. However, the needs of each organization are unique. Therefore, the reader should keep in mind that these are guidelines and should take their company's needs into consideration.

What is incident response

Incident response can be defined, in simple terms, as the process of addressing network events. This process can be both proactive and reactive. A network event can be considered any event that affects the confidentiality, integrity and/or the availability of information.

Most corporations have experienced events that have required some individual, or groups of individuals, to respond to adverse conditions on their networks. Unfortunately, most corporations do not have, or recognize a need for a formalized group of employees who are empowered to respond or protect against these incidents.

Where is the CSIRT

The Computer Security Incident Response Team (CSIRT) is a group of people that coordinates and supports the incident response efforts of a corporation. There are several reasons why this organization does not exist in many businesses today. Most of these reasons can be categorized as misunderstanding the purpose of the CSIRT.

The general support and maintenance associated with keeping a network running will usually receive a higher priority over protecting the organization against viruses or worms. Because of this, security is usually left to the network and system administrators. Often times, these individuals have other day-to-day tasks that cause security to be less of a priority. Also, they may not have the proper training to perform the security related tasks.

Even after an event such as the "I Love You" incident, many organizations did not create a formal CSIRT to help prevent and combat future incidents. This is because of the perception that security is a police force or "big brother" in nature. This means

management would probably be less willing to institute this kind of group.

Also, since people generally see security measures as inhibiting rather than enabling, executives are not interested in any process that can reduce employee productivity. This leads to an environment where incident response is addressed in an ad-hoc fashion. However, this may cause more harm than good.

When the CSIRT is missing, chaos rules

Since relying on network incidents is no guarantee that a company will create a CSIRT, other methods usually evolve. One common approach is for a group people, usually Information Technology employees, to recognize the need for security with an organization. They will usually implement security measures and respond to a network incident on a volunteer basis.

While this is better than nothing, this does not adequately solve the problems associated with incident response. Often times, these volunteers can become confused on how to proceed. This may create an uncoordinated effort, which could do as much harm as the incident itself.

Order from chaos

So, the first step in creating a formal CSIRT organization within a corporation is to convince management that security measures and incident response procedures are not inhibitive, but rather enablers of business. In other words, for a CSIRT to be successful there must be empowerment from the executive level of the organization.

The exact method of accomplishing this will vary from one organization to another, but they will generally involve the concept of sponsorship. High ranking IT managers, who support the CSIRT concept, should approach other high ranking mangers from the various business units. Once their buy-in has been received, together they can approach the Board of Executives and present the CSIRT concept. It is usually easier to convince the Board to spend money on overhead functions with the support of other business units, primarily the profit centers of the company.

Again, these techniques will vary; however, the concept of sponsorship of the CSIRT by the business managers is based on the general principle that the CSIRT will need the support of its constituency to get off the ground. In return, the CSIRT will "serve and protect" the constituency to the best of its ability against network incidents, which may cause downtime, missed deadlines, and unhappy customers.

Key Components

Once the company executives have officially approved the existence of the CSIRT, a.k.a – provided funding, the persons in charge of organizing it should be certain to address key components of what makes an effective CSIRT.

First, and perhaps foremost, is the relationship with the constituency. They are the people that the CSIRT are here to serve. Therefore, a clear and precise method of communication must be established. After all, how effective can it be if the community does not know how to relate to them, or worse, that they even exist!

The communication channel will involve several components, the least of which should be a central location for information, such as a web site. This site would contain information regarding policies, procedures, contact information, the purpose of the CSIRT, and statistics regarding incidents. Whatever the method, operating in a cloak-and-dagger approach should be avoided. This will most likely create an atmosphere of mistrust. The community should feel comfortable when dealing with the CSIRT.

Also, the CSIRT can hold functions such as training classes or seminars to help inform the user community about security risks. These events would serve two purposes. First, the constituency would be receiving a level of training they most likely would not receive elsewhere. It would help to raise their level of awareness, which may prevent some future incidents from occurring, or being as widespread when they do occur.

Secondly, it would help to enforce the communication line between the CSIRT and the user community. For any CSIRT to be effective, it needs information and strong, positive communications with its constituency. It would also help to prevent the "ivory tower" mentality. The purpose of the CSIRT is to enable business by protecting it. That would be hard to accomplish if they were isolated from the business people of the company.

Another line of communication the corporate CSIRT should explore would be communication with other, external CSIRTs. For example, a company CSIRT may work in conjunction with the national CSIRT. However, many companies are not quick to advertise their network incidents. Any communications along these lines should be approved by the company executives and handled by an authorized spokesperson. And of course, the communications need to be secured.

Once a clear method of communication has been established, the CSIRT must then disseminate information. There are several issues they can discuss with the user community regarding network incidents.

Probably good starting point would be to inform the user community as to the objectives of the CSIRT. These objectives should be clearly defined and written such that they are not ambiguous or require a high level of technical training.

Next, the services provided by the CSIRT should be explained. While these are probably going to vary somewhat from one organization to another, the guidelines set forth in RFC 2350 suggest a good, general starting point. As discussed below, this RFC suggests a guideline that can be used and modified to fit the needs specific to each organization.

RFC 2350 suggests that a CSIRT can be thought of as providing two basic services. They are incident response and proactive measures to prevent network incidents. Incident response can be categorized into three areas. They are incident handling, incident coordination, and incident resolution. Proactive measures are not necessarily required, but can help to better protect the company as a whole.

Incident handling, or incident triage per RFC 2350, refers to the process of assessing and verifying incoming reports regarding network incidents. In reality, some users may report "incidents" that turn out to be related to the fact that a printer is out of paper. Of course, the CSIRT could help reduce these types of reports by clearing communicating what constitutes an incident, however, reports that turn out to be false may still occur.

Once a report is verified and deemed to be a true network incident, the CSIRT will be responsible for coordinating the efforts to handle the incident. Incident coordination will be crucial in effectively combating network incidents. In the volunteer model, organizations were at risk of volunteers who did not communicate completely with the user community. The CSIRT will have formal procedures in place to handle communications. They should have the enough information to categorize and contact the appropriate personal regarding the network incident. The policy governing incident coordination should be clearly outlined and accessible through the communication medium of the CSIRT.

The third component of incident response is the resolution phase. Incident resolution is the process of implementing the procedure to stop and correct actions committed during the network incident. The CSIRT may have a limited role in this effort, or may be completely responsible for the cleanup effort. This will depend upon the organization's needs. In either case, the CSIRT should be able to advise any technicians working on the incident resolution phase.

The second service offered by a CSIRT, generally classified as proactive measures, can be crucial in helping to prevent network incidents. This is not a key operational necessity of the CSIRT, but can be extremely beneficial to the organization as a whole. Some of these measures outlined in RFC 2350 are:

- Information provision or archiving
    - This means the CSIRT will keep a repository of known vulnerabilities, patches, etc that can be referenced for educational or research purposes.
- Security Tools
    - The CSIRT will be able to research the latest security tools and

recommend methods for performing security audits. They may recommend a security toolkit to be used to conduct a comprehensive audit of a site or network.

- Education and Training
    - This will help to maintain user awareness and facilitate communications between the CSIRT and its constituency.
- Product Evaluation
    - As with security tools, the CSIRT can evaluate products and recommend their viability or configuration to meet company security standards.

- Site security – Auditing and consulting
    - Since the CSIRT will most likely contain the trained security experts within the organization, they will be able to perform as security consultants when the need arises.
    - Auditing is important to help maintain the security measures recommended by the CSIRT. Without accurate and timely audits, network incidents may occur simply because no one was paying attention.

As mentioned above, these are merely examples of proactive measures that may be performed by the CSIRT. However, they are not a required function. Also, keep in mind that the list above is merely a guideline. Some organizations may require more or less items to implement their proactive measures.

In some cases, it may make more sense to have a separate body performing some of these actions. For example, there may be a separate auditing group already in existence that can work with the CSIRT when performing security audits. It is important to remember that the CSIRT should be configured to meet the company's needs, which is enabling the business processes while protecting its information.

Summary

Many corporations today do not have an official response mechanism, or CSIRT, in place. This is true despite the several incidents that occurred during the years 2000 and 2001. Mainly, this is due to the misconception of the security process as inhibitive.

To successfully develop as CSIRT within an organization, the executive management structure of a company must empower the employees to act on behalf of the company during a network incident. Once this has been achieved, the CSIRT must develop itself into a professional organization the user community, or constituency, can turn to during a time of need.

Proper communication is a fundamental piece to the success of the CSIRT. Without it, they will be unable to adequately serve the organization in the role of incident response. They must operate with clear objectives and establish policies to govern their services.

These policies and services should be clearly outlined and available to the user community for informational purposes.

A majority of the work in the area of incident response will be political in nature as opposed to technical. It is important to keep this in mind, since the success or failure of a CSIRT will not only depend upon their technical expertise, but the ability to demonstrate its usefulness to management as an enabling process, not a restrictive one.

References:

Brownlee, N. and Guttman, E. "Expectations for Computer Security Incident Response" RFC 2350 June 1998 http://www.ietf.org/rfc/rfc2350.txt (6 Sep. 2001)

"Minimizing Your Potential Vulnerability and Enhancing Effective Response" http://www.nipc.gov/incident/incident3.htm (8 Sep. 2001)

Radcliff, Deborah "Overcoming Insecurity" Computerworld July 17, 2000 http://www.computerworld.com/cwi/story/0,1199,NAV47_STO47143,00.html (6 Sep. 2001)

West-Brown, Moria "Avoiding the Trial-By-Fire Approach to Security Incidents" Security Matters March 1999 http://interactive.sei.cmu.edu/news@sei/columns/security_matters/1999/mar/security_matters.htm (7 Sep. 2001)

West-Brown, Moria, Stikvoort, Don, and kossakowski, Klaus-Peter "Handbook for Computer Security Incident Response Teams" December 1998 http://www.sei.cmu.edu/pub/documents/98.reports/pdf/98hb001.pdf (7 Sep. 2001)

Note: The link above is active, but may not work correctly if launched from within Office XP.

Last Updated: May 27th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event