Incident Response in A Global Environment

Linda Kelver
GSEC Version 1.2b

Introduction

An incident is the unauthorized access, entry or attempt at entry to an information system. Some examples of possible incident categories include: compromise of system integrity; denial of system resources; illegal access to a system (either a penetration or an intrusion); malicious use of system resources, or any kind of damage to a system. Some possible scenarios for security incidents are:

- A strange process running and accumulating a lot of CPU time
- An intruder logged into your system
- A virus has infected your system
- Someone from a remote site is trying to penetrate the system
- The corporate web site has been defaced

A six-step process for incident handling includes: prepare, detect, contain, eradicate, recover and lessons learned. Technical staffs and support teams throughout the world execute the four middle steps – detect, contain, eradicate and recover – routinely, often without documentation to guide them. They just do it. However preparing an incident response procedure and team is not as universal.

The purpose of this writing is to share one company's experience in working the first step: establishing an Incident Response Team and Procedure and doing so in a "Follow the Sun" technology support environment.

Set the Stage

The organization has three technology centers in multiple time zones and a workforce in which someone is working around the clock somewhere in the world. The largest technology support center is in the US, a second support center is 6 hours later in Europe and a third support center is 13 – 16 hours later in Australia. These three centers are charged with supporting the organization's technology requests in an environment where most employees work a typical Monday – Friday, but some employees are on the job during weekend hours as well.

In May 2000, when the ILOVEYOU virus was released, the European center heard the news first and informed its US counterpart of the virus, a few hours before the US awoke. So the US mail administrator was able to stop the virus at the mail gateway before Exchange e-mail systems in the US started flooding networks with this virus. With the increase in virus outbreaks, the organization pressed for a global procedure to deal more adeptly with viruses and other security incidents.

Identify the Team and Goal

A Security Incident Response Team is a group of professionals in the organization who are trained to respond to a serious security incident. This team's role is investigative and problem solving. It should include management personnel with the authority to act; it should have technical personnel with the knowledge and expertise to rapidly diagnose and resolve problems; it should have communications representatives who can keep the appropriate individuals and organizations informed on the status of the problem and to develop public image control strategies as necessary.

The composition of the Incident Response team and the circumstances in which it is activated should be clearly defined. The team should be available and on call in emergency situations and should have the authority to make decisions in real time, not bound to bureaucratic levels of approval and decision-making. Procedures that define the circumstances under which the Team is activated must be clear.

Activation for every simple incident, such as an employee's keying error, can be wasteful and time-consuming. However, if a serious incident, such as an intrusion attack, is in progress, delaying the activation of the Team could result in serious damage to the company's information assets and supporting information systems. Therefore activation should be considered only when information systems must be protected against serious compromise, --- an unexpected, unplanned situation that requires immediate, extraordinary and fast action to prevent a serious loss of information assets and/or mission capability. The planning process should consider which Team members will be needed for different levels of incidents, and how they are to be contacted when an emergency occurs.

Management representatives from the three support centers were included as well as senior technical resources. The goal for this group was to define an incident response procedure that could be quickly deployed and easily followed. Additionally we had to develop a corporate communication plan that we could rapidly deploy if necessary.

Challenges

Primary challenges in developing a global procedure were:

- Time differences
- Three different Customer Assistance functions with three different systems for reporting problems
- Labor laws differ around the world, sometimes preventing personnel from working second and third shifts and weekends
- Keeping three regions in communication loop
- Timely communication to central point of contact in US
- Providing timely global communication when necessary
- Level of trust among technical staffs in the three regions

Developing the Procedure

Because of distance and time differences, we did not have a meeting with all team members present. Rather we teleconferenced with either the European group or with the Australian group to discuss issues, but relied heavily on e-mail to share documents. A 'straw' procedure was presented and over a period of several weeks it was refined to the point of being ready to test.

Some key incidents were identified and scripted to assist the CA groups in determining if a reported problem might rise to the level of an incident. If a certain level were reached, CA would notify a contact from the Services group. The responsibility for making decisions about escalating and informing other regions lies both with the region in which the incident occurs and the Security Office.

All CA groups were put on a notification list to receive virus alerts from the company's anti-virus software provider. Security personnel from the US and their pagers were put in a group mail list; if an incident rises to the level of notification, the CA sends a formatted message with the incident type in the subject. The body of the message has a brief description of the incident. For a virus, they include the name of the virus and what part of the system it's affecting.
Each region's Operations Support has a cell phone that is monitored 24-7and all regions know the number. This cell phone is the method of contact for Operations Support, both within the region and globally.

Sources of Information for the Team
Customer Assistance procedures contain links to virus sites so they can check for hoaxes and for viruses. If there's a virus incident for a documented virus, Customer Assistance goes to the link to get information about the virus for communication.
http://www.icsa.net/services/consortia/anti-virus/alerthoax.shtml
http://www.datafellows.com/news/hoax.htm
http://www.symantec.com/avcenter/hoax.html

http://www.it-secure.com/Links/incident.htm contains links about hacker attacks, new viruses and various computer incidents.

The Procedure: Assess, React, Communicate
A call comes in to the Customer Assistance office for a region. The Customer Assistance agent uses the script to determine if the call is a potential security incident. If it is, the agent engages the Operations Support duty officer who collaborates with the Global Security office if necessary in determining the level of concern. For an incident, the technical lead is engaged to determine the level of concern both regionally and globally.

While the technical team is engaged in fully assessing and reacting to the incident, the Operations Support duty officer and Global Security Office consider communication to other areas: if the incident is potentially global in nature, the other regions' duty officers are contacted. If the incident has legal or law enforcement ramifications, the Global Security Office engages Internal Audit, senior management and law enforcement. And if there is a need to inform employees of the matter, there's a template that has been pre-approved. Customer Assistance will customize the template and send it to Communications with a priority for publication.

If it's necessary to communicate with facilities throughout the world, there's a Customer Relations lead in each of the three regions. This lead has a list of key contacts in their region and will communicate with them.

Table 1 shows the operational view of the incident team

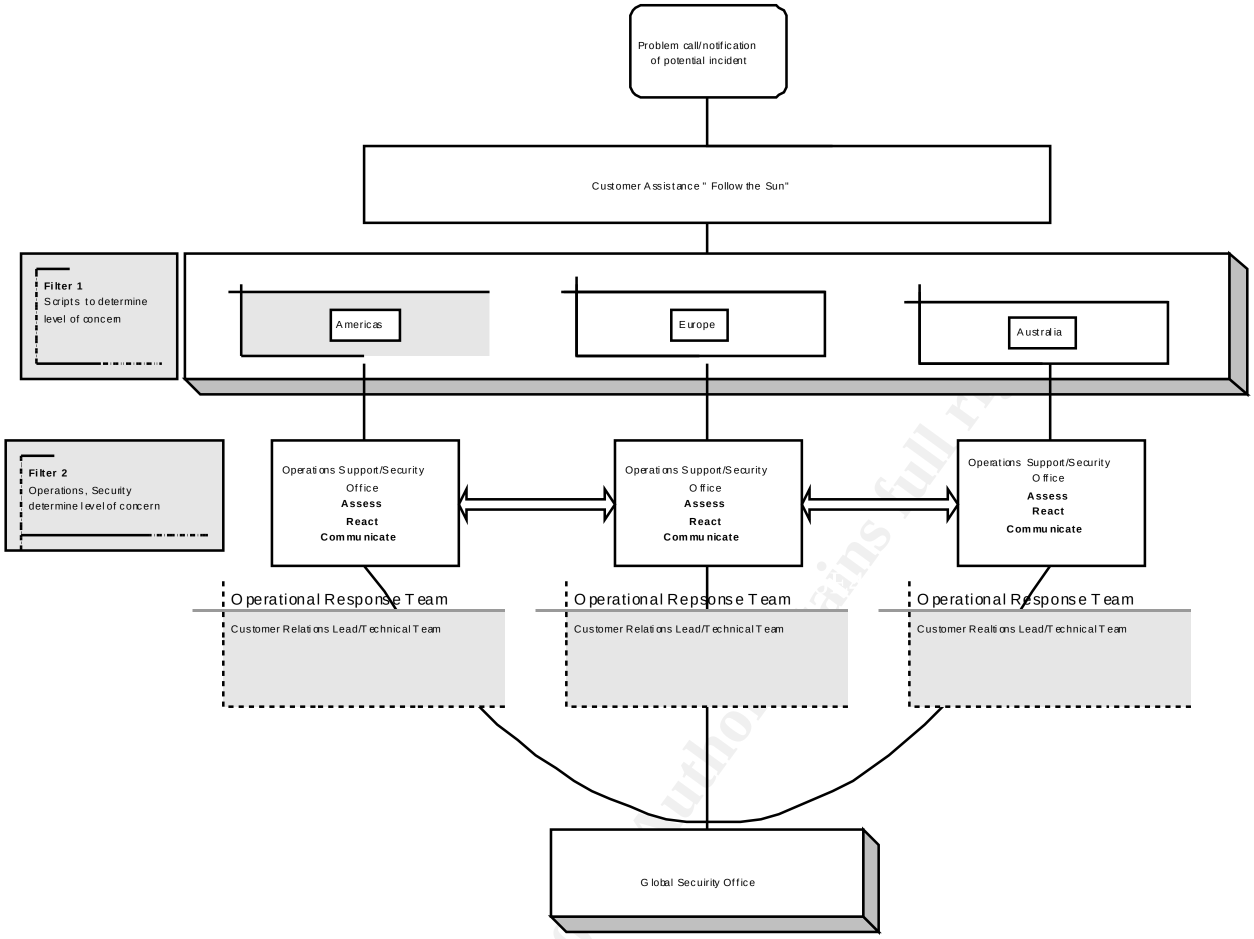

Table 1

Support in the Off Duty Hours

The technical team in the US, because it is always on call, determined what access would be required in order to protect the corporate network if an incident occurred in another region during off duty hours. A procedure was created to safeguard these high level accesses. Once the accesses were established, the US team tested them followed the procedure to use the ids, documented their use and had the passwords reset. .

This proved most challenging because of the level of trust between regions. Administrators typically don't want anyone to have access to their system/network/firewall/servers. But because labor laws differ globally and because of global staffing shortages, the US technical staff is expected to react to emergencies regardless of time of day, day of week and holidays.

Test the Procedure

A 'trumped up' virus was used to test the communications component of the incident handling procedure. This test proved the effectiveness of the e-mail/pager notification of the Security staff on call. It found a flaw in the duty officer phone list, but did prove that the bare bones of the procedure worked. The US had live tests on various occasions with virus incidents soon after the procedure was developed and it was refined based on these test results.

The procedure is available on the company's intranet site and is maintained by the Global Security Office.

Document/ Lessons Learned
It is imperative that the Response Team learns from each incident. The incident response procedure should be updated with lessons learned. Since each region has its own problem tracking system, the Security Office pulls documentation from the responsible region's problem system, adding notes the technical staff makes. A post mortem meeting is held to discuss what worked, what didn't, and how to improve.

The procedure is reviewed quarterly and updated as personnel and processes change. It is the responsibility of the various technical support areas to ensure that technical staff is familiar with the procedure but the Security Office is responsible for annual follow up to gauge effectiveness of the procedure.

Summary
The challenge in developing a global incident response procedure with global buy-in and management support was met by starting with a basic incident response framework. We used the Operational "Follow the Sun" model to ensure that someone would always be on call and would have the supporting structure to react to an incident regardless of where and when an incident originated.

Once the team was identified, roles documented, scenarios developed, work flow and communication flow documented, the procedure was tested in all three regions. The region with 24-7 responsibility requested access that would permit basic network/system protection In the event of an incident. The incident procedure is reviewed, updated and tested periodically.

References

DEPARTMENTAL GUIDE TO INCIDENT HANDLING PLANNING, U.S. DEPARTMENT OF TRANSPORTATION, OFFICE OF THE SECRETARY, URL: http://cio.ost.dot.gov/InfoAssurance/HTML/DOT_H1350.255.HTML#_Toc450961704

Carnegie-Mellon Software Engineering Institute, "Responding to Intrusions", URL:http://www.cert.org/security-improvement/modules/m06.html

CSIRT.WS, URL: http://www.csirt.ws/csirt/index.htm

Northcutt, Stephen, Computer Security Incident Handling Step By Step Guide, v1.5, The SANS Institute, May, 1998

Radcliffe, Deborah, "Overcoming Insecurity", 7/17/2000
URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO47143,00.html