Global Information Assurance Certification Paper

Computer Security Incident Response Procedures - do you need one? You bet you do!

Katherine Bursese
January 16, 2005

For ease of writing I will refer to Computer Security Incident Response Procedures as CSIRP's for the remainder of this document.

I would like to describe an incident that occurred at a well-known technical university that clearly shows the need to have an enforceable and workable CSIRP.

> **Picture this; it is 1am and email comes into the security mailing list from an outside source informing us that this sites server has been compromised and from the logs two of the machines in our domain look to also have been compromised. The only people on the mailing list that are up and awake and reading their mail are the Operations staff but they know that sometimes in the wee hours one of the more nocturnal network staff come in. They take a chance and call his office. To their delight he IS in his office, so they forward him the security email and consider their part of this incident finished.**
>
> **The nocturnal network person reads the email, looks at the time and decides to block those 2 hosts at the router from the Internet. He then sends email to security stating that the hosts are blocked and considers his part in this incident finished.**
>
> **The next morning the rest of the security team trickles in and reads the security mail along with about 500 other emails of various severities. 100% of the team makes the assumption that the Nocturnal Network person notified the owner of the machines of the problem and action has been taken. We all get on with other business and of course the Nocturnal Network person being Nocturnal is not around in the daylight hours to correct our assumptions.**

Outcome:

The two servers that were blocked were two major servers for the math department. They both had off site collaborative projects going on of a high profile nature. The math department has their own System Administrators that were NOT on the security mailing list.

The sys administrators spent all of that day and part of the next troubleshooting their server and network trying to figure out why they could not get to the Internet. (Insert Jeopardy buzzer sound here) No one informed the owners of the alleged compromised hosts of the network block or the alleged compromise until the problem was elevated to the Director of Networking and the Chair of the Math Department!

Where to start is the first question that comes to mind. SANS has a wonderful Booklet that not only outlines the key elements for a successful CSIRP but also includes forms that can be used to identify the Incident Contact Personnel as well as forms for Incident Handling, Containment and Eradication. This publication can be ordered online and a site license can be obtained for copying and distribution of the forms.

The next excellent source of information when attempting to create a successful CSIRP is the Handbook for Computer Security Incident Response Teams from Carnegie Mellon/Software Engineering Institute. This is a large document but also is very thorough and I found it to be an excellent resource when drafting our CSIRP. This manual also offers helpful templates for recording information and contact people.

Not having an Incident Response policy can lead to serious liabilities for your company or university as well as the System Administrator that is working on the incident. There may be times when local law enforcement will pay you a visit and it is a very good idea to know what information can be given out without a search warrant and in the case of a warrant who in your organization should receive the warrant. Knowing someone in your local Computer Crimes Lab is a good idea. Having good communications with them BEFORE you are responding to a critical incident will make life much easier.

The FBI has developed a collaborative effort named InfraGuard. This a description of the organization taken from their web page:

> **"InfraGard is a cooperative undertaking between the Federal Bureau of Investigation and an association of businesses, academic institutions state and local law enforcement agencies, and other participants that is dedicated to increasing the security of the critical infrastructures of the United States of America".**

This organization has proven to be extremely valuable to me in learning about Computer Forensics and well as allowing me to network with many of the law officers in the computer crime lab. My organization has joined InfraGard and I serve on the board of directors of our local Chapter.

It is also critical to have someone assigned to notifying and reporting incidences to CERT. This can be called out in your CSIRP clearly so everyone knows what they are responsible for and you can cut down on redundant reporting.

And last but certainly not least, let's not forget that an ounce of prevention is worth a pound of cure. Educating your user community will help decrease the amount of Security Incidents you will have. It's been proven time and time again that most security problems originate from INSIDE your organization.

Having a clear and concise Conditions of Use policy as well as a Policy for departmental computers on your network will prove invaluable resolving internal security violations.

When developing your policy a lot will depend on what type of organization you work at. Government policies differ drastically from Private Sector Policies and university policies are also in their own category, being even more specific depending on if they are public or private institutions.

If you don't think you need a CSIR policy, I challenge you to the following exercise Do a mock incident (with the permission of your management), but don't let your security people know it is an exercise. If all the bases I have covered in this paper are taken into consideration in a clear and calm manner without a CSIRP please send me an email, I want to electronically shake your hand!

The difficult part of creating a CSIRP is that it has to be tailored for your site. The sources I have cited in this paper will be of great assistance but you won't find a ready to use policy there. You will need to take into consideration all the nuances of your particular site as well as getting support and buy in from upper management.

Best of luck to you, it will be well worth the work I guarantee you.

SOURCES

SANS Home page
URL: http://www.sans.org/newlook/home.htm

Moira J. West- Brown Don Stikvoort Klaus- Peter Kossakowski "Handbook for Computer Security Incident Response Teams (CSIRTs)"
December 1998 HANDBOOK CMU/ SEI- 98- HB- 001 Pittsburgh,
PA 15213- 3890
URL: http://www.sei.cmu.edu/pub/documents/98.reports/pdf/98hb001.pdf

InfraGard
URL: http://www.columbus.oh.us/infragard/

Computer Emergency Response Team (CERT), Coordination Center URL: http://www.cert.org/index.html

Defense Information Systems Agency - DISA Information Assurance Program Management Office
URL: http://www.disa.mil/infosec/

Marjorie W. Hodges and Steven L. Worona. "Legal Underpinnings for Creating Campus Computer Policies" - Winter 1996, v19n4, p5-9)
URL: http://www.educause.edu/pub/ce/cause-effect.html