Global Information Assurance Certification Paper

Establishing a Computer Incident Response Capability at a University

GSEC Practical Requirement v.1.2d
By Clyde Laushey
May 28, 2001

Purpose

This document will attempt to describe several of the problems you may encounter when establishing and operating an incident response capability that are unique to a university environment. Some ideas for dealing with the problems will be suggested but it must be noted that several of these problems are somewhat inherent to the environment and might elude a good solution for some time.

Introduction

It is now generally well accepted that all organizations require some sort of computer incident response capability. Failure to provide such a capability could be considered legally negligent. It has been argued that organizations may be held liable for damages if their computer systems are used in denial of service attacks and security best practices were not in place or followed.

Universities are certainly not immune from these obligations. However, there are a number of special circumstances at a typical university that can make establishing and operating a computer incident response capability very challenging. Investigating incidents can be an especially sensitive area of concern. There are some issues dealing with the privacy and security of student information that do not have an exact parallel in the business world.

Current Best Practices

Best practices in the area of planning, developing and operating a CSIRT (Computer Security Incident Response Team) have been described in detail in a number of excellent documents available on the Internet. For specific information, please refer to any of the following sources (see the "References" section below for additional information needed to access a specific document).

- "Handbook for Computer Security Incident Response Teams (CSIRTs)" published by The Software Engineering Institute of Carnegie-Mellon University. The SEI is closely affiliated with the CERT/CC (Computer Emergency Response Team/ Coordination Center) which is considered one of the leading authorities in the world concerning computer security and incident response.
- "Establishing a Computer Security Incident Response Capability (CSIRC)" published

by the Computer Systems Laboratory (CSL) of the National Institute of Standards and Technology (NIST). NIST also publishes a document entitled "An Introduction to Computer Security: The NIST Handbook" which is an excellent introductory text covering all aspects of computer security (including incident response).

- RFC 2350: "Expectations for Computer Security Incident Response" which is an Internet standard in the area of "Best Current Practice". "RFC" stands for "Request For Comments" and is the vehicle by which Internet standards are reviewed and approved. Note that an organization's adherence to "best practices" will probably be the legal measure used in determining if reasonable due care was exercised in dealing with an incident. It is only a matter of time before an organization is sued for failure to adequately protect its information assets and respond to an incident.
- RFC 2196: "Site Security Handbook" which is in the "Informational" area.
- "Forming an Incident Response Security Team" published by the Australian CERT. This document addresses many of the issues related to developing a CSIRT within a university environment; many of the issues dealt with are also applicable to other types of organizations with limited budgets and staff.
- "Computer Security: Incident Handling Step-by-Step" published by The SANS Institute. There is a charge for this reference but it is the best example of a practical, "how to" treatment of incident response.

Problems Specific to the University Environment

The following points are not within the exclusive domain of universities. Many of these will be encountered in all sorts of organizations. But they tend to dominate the process at most universities and if not considered will probably result in the failure of the effort to develop an incident response capability.

Openness and intellectual exploration are considered to be more important than computer security. Students are inherently inquisitive and some will tend to want to explore the computer systems they have access to. Arguments are often made that what information security practitioners would consider to be hacking should be allowed (or at least tolerated) as part of the student's education. Note that the faculty members can often be more inquisitive than the students are. There are many "gray areas" within the computing domain and when there is a disagreement about whether an activity should be allowed or not, universities tend to err on the side of openness and intellectual freedom. An important point to remember is that you will encounter both faculty and students who are unusually intelligent and even gifted in the area of computer programming. The individual you might be trying to stop could very well be the author of one of the tools you are currently using to try to stop him.

There are thousands (and sometimes tens of thousands) of students with almost unlimited access to very high-speed networks. They will also usually have access to every piece of software for which there is a known vulnerability. And they often have a lot of free time

on their hands.

There tend to be many individual systems that are outside the control of any sort of central data processing organization (where a CSIRT would reside) but which are still connected to the university's network. Businesses can experience this also but it can be taken to an extreme at universities. It is not unusual to encounter hundreds of servers running dozens of different operating systems and every networking protocol currently available. Almost every known vulnerability that exists at any given point in time can be found on a university server; and the odds are that the fix has not yet been applied. This situation can often result in a large number of relatively inexperienced system administrators for whom security is the least of their concerns. System administration may not even be their primary job duty. They may have received no formal training in security or even in general system administration. They have neither the time nor the expertise to secure their systems - they are too busy just trying to keep the computers up and working.

It can be difficult to gain strong support for the establishment of security policies, procedures and guidelines. Universities operate more by consensus than do most businesses; dictating policy is not normally the method used. Policy making at a university is typically a long and very slow process. There can be extended debate over seemingly minor changes to the wording of a document. Even when support can be obtained "on paper" real support may not actually be available. It will often take a visible incident to prompt any real support and cooperation. Without a written security policy with related procedures and solid university backing, running a CSIRT is probably pointless.

Universities have an unusually diverse constituency which includes faculty, staff, students (fulltime, part time, day, night, undergraduate, graduate, distance), contractors, faculty business associates, visiting scholars, etc.). It can be almost impossible to communicate with the entire university community via electronic or other means. A for-profit business can more easily mandate that all employees will have an email account and will read email at least once a day. Such a mandate would almost certainly not be made at a university and even if it were, it would be almost impossible to enforce. This problem with mass communication to the entire university community can be a surprisingly difficult one to solve. The politics involved in sending a mass emailing to all members of the community can be almost overwhelming; and not everyone will have a university email address that they use regularly. Printed mailings are much too slow for dealing with security matters. It is almost impossible to encourage everyone to review selected web pages on a regular basis. There is not a simple solution to this problem.

There is a culture of extreme independence at universities, especially among the faculty. This attitude seems to go hand-in-hand with the desire for intellectual exploration that is obviously necessary for scholarship. Unfortunately it can sometimes translate into an "I will not be told what to do" mindset which can make investigating a security incident much more difficult than necessary. As an example, at my institution a critical system

was hacked (i.e., defaced web pages, rootkit installed) and central IT was not able to persuade the owner of the system to change all passwords. He said that this would be too inconvenient to the faculty and would delay their progress; there was a definite implication that they did not want to be told what to do.

There is also a culture of both intellectual and personal privacy that can add to the difficulty of investigating an incident. A faculty member who is doing leading edge research may not want the CSIRT (or anyone for that matter) examining his PC for evidence of an incident. This is somewhat understandable but it does make the investigation more difficult. Generally accepted forensic techniques such as physically securing the site of an incident for some period of time while the investigation takes place would be difficult if not impossible to do. There is also a certain amount of mistrust between the faculty and staff (the most likely members of the CSIRT) at most universities; this is unfortunate but it is often the case. When a staff member of the CSIRT requests access to a faculty member's PC, the response is very likely to be "No". Due to the dual reporting structures for Academics and Administrators at most universities, there will not be much the staff investigator can do about this situation.

Universities (and especially public universities) are often faced with tight funding and this can make it very difficult to obtain dollars for IT security staff, products, services, training, etc. It is more difficult to make the case that security supports the mission of a public university than it is for a profit making business. There is not a good solution to this problem since there is an element of truth to the point.

Additional FTE's (i.e., Full Time Employees) can be even more difficult to obtain than funding. This can often mean that participation in the CSIRT is voluntary and restricted to normal working hours (i.e., no pagers). The members of the CSIRT may be participating on an "as time permits" basis which is not really a workable solution. The leader of the CSIRT, who is most likely the institution's Information Systems Security Officer (ISSO), may be the only member of the team who deals with security fulltime. The other members of the team may have no security training other than what they have learned on the job. The ISSO will probably not have any line authority over the other members of the team and will have to use persuasion to get things done. This will slow down any investigation considerably. During certain times of the year, it could make investigation all but impossible.

There are a number of federal laws and regulations related to the privacy and security of student information which can make investigation of an incident much more sensitive than usual. For example, the Family Educational Rights and Privacy Act of 1974 (FERPA) requires that students be advised of their rights concerning certain personal or Education Records maintained by an institution or by a party acting on behalf of that institution. It could easily be argued that a student must be notified that he is being investigated for an incident before the investigation begins. It can be very tricky for the members of the CSIRT even to communicate among themselves about the specifics of an investigation; it could be considered a violation of FERPA to reference a student's name

in any written communication. Issues of this nature have not yet made their way to the court system so they are still very much a "gray area". Most universities will take the position that they should err on the side of more protection of student information rather than less.

Most of the members of the university community honestly don't care about computer security; they don't see what it has to do with their specific mission and consider it nothing more than a hindrance. This is a common problem at most organizations of any type and is the reason why security awareness programs are considered a cornerstone of any effective security program. But at universities, intellectual exploration and inquisitiveness is so much more important to the overall mission that this ambivalence towards security is understandable. Universities need people who love learning and sharing what they learn; this mindset is somewhat counter to effective security. It is their nature to create new knowledge, share that knowledge with peers and teach it to students. Anything which makes that harder to do is "a bad thing".

Conclusion

None of the problems listed above are trivial to solve; some are unsolvable without a fair amount of pain. When planning and establishing a CSIRT in a university environment, keep the following points in mind.

With a rare few exceptions, a university is simply not going to be as secure as a profit making business or a critical governmental agency. Our mission critical priorities are different and some of them conflict directly with security.

Resources, both staff and funding, will always be inadequate to the task (at least as the ISSO sees it). Incident response will involve juggling priorities and trying to get the most value from the money and effort expended. This will require good planning upfront and some difficult decisions concerning priorities after the CSIRT is in place.

Always try to work from a consensus, especially when developing policy and procedure, building the incident response capability and developing an awareness program. An actual incident response must be conducted according to a strict set of rules and guidelines but these should have been developed earlier by consensus. If you deviate from this suggestion, you will most likely not have the support of the community. The more people you can involve in the process, the more likely you will succeed. Try to involve everyone who expresses any interest in the process.

Strive to make security as invisible to the end user as possible. Procedures that can be mandated in a business will more often than not be rejected in a university setting. Security measures cannot be seen as a hindrance to any sort of intellectual pursuit or they will be ignored. One suggestion when trying to sell the program to the faculty is to

describe security as a tool to protect their "intellectual property". The ultimate goal of scholarship is to share your work with others - but not until it has been completed! Most faculty members simply do not know how insecure their computers are; if you can illustrate this point to them, you can gain their support.

It is critical that a solid risk assessment be carried out initially and updated on a regular basis. Due to the problems listed above and also the inherent difficulty of computer security, efforts must be directed towards protecting the university's most critical information assets. Assets must be evaluated from the perspective of the university as a whole and not from the perspective of one politically powerful faculty member. This may (and probably will) require more political skill than the typical ISSO possesses so attempt to solicit some help.

Finally, always remember that security is just not going to be a top priority for anyone at a university except for the ISSO. And that's probably the way it should be.

References

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

John P. Wack. "Establishing a Computer Security Incident Response Capability (CSIRC)". NIST Special Publication 800-3. November 1991. URL: http://csrc.nist.gov/publications/nistpubs/800-3/800-3.pdf

N. Brownlee, E. Guttman. RFC 2350: "Expectations for Computer Security Incident Response". RFC Category: Best Current Practice. June 1998. URL: http://www.rfc-editor.org/rfc/rfc2350.txt

B. Fraser. RFC 2196: "Site Security Handbook". RFC Category: Informational. September 1997. URL: http://www.rfc-editor.org/rfc/rfc2196.txt

Danny Smith. "Forming an Incident Response Team". Australian Computer Response Team. The University of Queensland. 1994. URL: http://www.auscert.org.au/Information/Auscert_info/Papers/Forming_an_Incident_Response_Team.html

Last Updated: May 26th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 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 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
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
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
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
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
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