Global Information Assurance Certification Paper

KISS: Keep It Secure Stupid

Everett Starnes

December 25, 2001

I have been working in Data Processing field for about twenty years now. I started out as a programmer. Security was not a big issue, except for user IDs and passwords, which were needed to logon to the main frame computer and the system administrator controlled them. Ten years later new words like LAN and WAN were becoming common in the work place. Security was becoming an issue. However security has been on the back burner, if not on the burner at all for many IT professionals. Like all good employees we did what we were told. 'Write a program to automate the filing process,' the boss would say. We wrote that program with alacrity without little or no thought about security. Many have paid the price and will continue to pay for software with security bugs and holes which compromise, computers, networks and organizations. In recent year as a system administrator, I was concern about keeping passwords secure. I also read the daily system logs, looking for anything suspicious. I backed up critical data daily, weekly, and monthly. There was even a Security Officer that worked in a different building. The Security Officer would email occasionally but I rarely talked to him. Knowing what I know now security was a farce. But lucky we had no incidents or should I say I wasn't aware of any incidents. Now at a different organization, for only four months now I am the Network Security Manager. Ever since then I have on the fast track on learning about network security. If you think IT employees are lacking in security knowledge, and we are. Imagine what non-IT employees know about security. Frightening isn't it. Yes. They are not aware of the consequences caused by certain actions. Most employees use technology to perform their jobs fast and efficiently. Security is often seen as a hindrance rather than as a necessity. A huge advertising effort is needed to improve security awareness on all levels.

KISS: Keep It Secure Stupid, is a simple phrase, perhaps but in everyday business many have not secured their systems in the first place let alone keep them secure once they take the precautions to secure them. Many IT professionals are either; over worked, ignorant, lazy, careless or negligent. In an environment such as this accidents are bound to happen. Not to mention all the malicious code, viruses, hackers and evil doers that are out there scanning and trying to penetrate a vulnerable system. When it comes to network security you can't leave anything to chance, or chances are that your network or personal computer on the network won't stand a chance of staying up and running as expected.

Over the years security attacks have taken many forms, from physical theft of computer equipment, password guessing and social engineering to IP Spoofing and distributed denial of service (DDOS). The old Unsophisticated attacks are just as prevalent as the newer attacks. Intruders are constantly scanning systems for known vulnerabilities and discovering new vulnerabilities. Knowledge of threats and IT security safeguards is inadequate in many organizations, because of the amount of time and perhaps money it takes to develop IT security. It is difficult to be fully informed as to all the old and newly discovered threats and the countermeasures that are necessary to thwart a threat. In many cases there is also uncertainty as to what security measures are appropriate to

counter all of the know threats. IT systems have been under attack for decades now, but never before were so many computers networked. Never before have so many cheap automated information attack weapons been available to would-be hackers. It is much easier for novice unsophisticated attackers to cause considerable damage. It is often impossible or very difficult to know if you are under attack and from whom. Attacker sophistication has increased enormously in the past couple of years. Become familiar with all the different type of security attacks. Learn all about your network and networking concepts.

Technology evolves so fast that vendors concentrate on time to market, not security. Until customers demand secure products, the situation is unlikely to change. Software and hardware is created with ease of use as the primary goal and security is often not considered. Products are so easy to install and operate that people with little technical knowledge are administering systems. Unfortunately, it is very difficult to configure a secure system. This alone is resulting in increasing number of vulnerable systems out in the wild of the Internet. Without the proper protection and security you are only making worse the already grave situation. Therefore IT professionals need to take steps to secure all technologies from known vulnerabilities. Organizations can secure their systems as great as they need to, but a minimum standard should be adhere to by all organizations.

Even the most vigilant, security-conscious organizations are very challenged to maintain IT security, especially after fixes, workarounds and new technology installed. The IT security group must put measures in place to protect information, systems and services which eliminate or reduce significant threats (disasters, mistakes, unauthorized manipulation of information, software and hardware and hackers) to an acceptable level.

Four major security issues concerning security are confidentiality, integrity, availability and authentication. Confidentiality: preventing the deliberate or accidental disclosure of sensitive information and processes. Data should remain private in storage and during transmission. Integrity: protecting automated information from deliberate or accidental corruption. To control modification to information and processes, data should remain accurate in storage and during transmission. Availability: protecting automated information resources from deliberate or accidental actions that would prevent information and services from being available when needed. Authentication: some times it may be necessary to be able to prove where information came from. This is called non repudiation. A sender may also require proof that the message was received by the intended receiver. encryption, digital signatures and challenge-response are some of the methods used to achieve secure communication. Organizations are vulnerable to internal and external attacks. All users from president of organization to newly employed intern, who may share a computer, have an organizational, ethical and should have a legal responsibility to protect sensitive information. Users play a vital roll in keeping your system secure.

Data security has three major layers for any type of organization or individual prevention, detection and recovery.

Prevention involves the avoidance of intrusions and related damages to hardware or software. Network protection is provided through either a software or hardware firewall. Prevent installation of unauthorized hardware. Even if care has been taken to provide protection through secured physical access, stringent authentication methods, updated anti-virus software, and properly configured firewalls, the possibility always exists that a way will be found to circumvent these protections. If that does happen, your next layer of defense is to be aware of it so you can react and minimize the damage.

Detection involves having the systems in place to provide awareness of intrusions or attempts when they occur in order to reduce their impact. This includes alerts and regular audits should be performed on each server, router, firewall, or other network device that supports event logging.

Recovery involves having the ability to undo any damage caused by a threat and returns information assets to a known operational state. It includes Data Backup, Operating System Software and Application Backup, and critical Hardware backup. Store backup tapes off site. Data Backup: maintain complete, current, and verified readable backups of data on media separate from servers. Create a restoration plan. Operating System Software and Application Backup: An item easily overlooked is ensuring that backups exist of the system software (network operating systems, router operating systems, etc.) and applications in addition to the data. Without these foundational pieces of the system, the data is unusable. In most cases these types of software can be repurchased or copied from another location, but the amount of time it may take to find and deliver the media may be unacceptable to the organization. The lost revenue may cause financial hardship and the company's image can also be damaged. In addition to the base software, all tested and applied patches should be available as well. It would be advisable to store these items in a manner similar to data. Hardware backup: Hardware critical to the day to day operation is on hand. This equipment can be use in a test area to test it and new software before you put it on your production hardware. A hot backup standby system is one redundancy approach that provide the immediate available if the primary system fails. A warm backup system requires some configuration before it can take over for the primary system. A cold backup need extensive configuration before being used. This equipment should be kept off site or at least away from the primary production equipment. Remember, data security and recovery plans need to ensure that spare hardware is available to replace damaged equipment. This includes servers, routers, and other infrastructure hardware that is essential to the organization's operations. The most difficult aspect of this element is funding. It is often difficult to convince those who must pay for this equipment that it is indeed necessary. The cost of downtime must be determined to provide justification for having capital invested in equipment that will not be used on a regular basis. If immediate repair is not required, standard or enhanced warranty terms may be sufficient that can ensure repair will occur within the needed timeframe.

A CIRT (Crisis Incident Response Team) or designated person(s) will analyze the scope of damage caused by an intrusion. Prevent further damage and return a clean system to normal operations. The CIRT is the source of all known security threats and remedies for

those threats and vulnerabilities. Collects all information on each an every incident and produces a formal report on each incident. Each incident is reviewed and a lessons learned document is updated with any new findings. Forensics may also be done by the CIRT if needed. Evidence is collected and protected in the event of legal proceedings against the intruder. An after action report of each incident is published for everyone in the organization to read. Evaluate, correlate and prioritize each report. Investigate each report or set or related reports. Work with any and all members of the organization to eliminate future incidents.

IT professionals can significantly reduce the likelihood that their networks will be compromised if they learn the infrastructure of their organization's entire network hardware and software. Create an inventory of the organizations hardware. Protect and keep this inventory up-to-date.

Establish a network security team, one person can't protect a system that is up and running 24 / 7. Security division will be responsible for developing and administering the organizations security program, including recommending and implementing security policies and procedures. Providing advice and assistance to various organizational personnel (technical and non-technical) in identifying security requirements for the different automated systems including security considerations in application development, implementation, operation and maintenance. Performing risk assessments and identifying potential security risks that may arise. Communicating security issues and concerns to agency management staff. Investigating security incidences and taking appropriate actions. Evaluating and recommending security products and solutions. Establish and allocate security responsibilities.

A network security policy must be created and management must be involved in creating and enforcing the network security policy. Everyone must read and sign an acknowledgement of reading the security policy at least once a year. Insure strict compliance with security policy. The best way to ensure that the security policy is adhere to and performed in a consistent and timely manner is the assignment of responsibility for each activity to a staff member or group, and to conduct regular audits verifying the accomplishment of these responsibilities. A person or group is responsible for developing, maintaining and enforcing all security policies. Conduct a legal review of all policies and procedures.

Create a user policy, distribute it and educate users. Create technical guidelines for the secure installation, maintenance and production of your servers and networks (or other perceived weak points). Audit sensitive systems regularly. Design a security awareness program that reflect and supports the mission of the organization. All employees must understand their responsibility in the organizations overall security goals. Employees must be aware of threats. Each employee must be held accountable if they break any security rules outline in the security policy and or user policy.

Educate and constantly train everyone in your organization so the security is second nature. Develop, implement and manage security awareness and training for users.

Install anti-virus software and insure updates are always up to date and all PC's are updated. Many anti-virus packages support automatic updates of virus definitions. It is recommended that you use these automatic updates when available. If you get a suspicious or unknown email attachment don't open it. It is not enough that the mail

originated from an address you recognize. Many viruses spread precisely because it originated from a familiar address. Malicious code might be distributed in amusing or enticing ways. Never run a program unless you know it to be authored by a person or company that you trust. Also, don't send programs of unknown origin to your friends or coworkers simply because they are amusing -- they might contain a Trojan horse program. Set up a firewall and disable all unused services and assess all network protocols. Set up an Intrusion Detection System. (IDS) Review the daily logs and put alarms in place to go off if any abnormal activities are detected. Put systematic security incident reporting procedures in place. Protect all logs. Create a CIRT (Crisis Incident Response Team). Install latest patches for all your software. Read the manuals or browse the vendor's web site for more information. Some applications will automatically check for available updates, and many vendors offer automatic notification of updates via a mailing list. Establish secure remote connections for the network. Employ multiple layers of security this ensures no single point of failure. Secure public web servers. Web sites are important for organizations to publish information, interact with web users, and or conduct e-commerce business. We all have heard of a least one organization that had their web page defaced. Organizations could loss money when the contents of their web pages are change by intruders. Classify information. Recognize what information is most important. Daily research to find any new exploit and have and a system of reporting pertinent information to all in the organization. Educate your network security team on new technology and how to secure this new technology before it is put in use. Stay current of latest developments through vendor web sites, CERT web site and web sites of network security agencies. Ensure proper security measures are always used when disposing of a system. All this said management and IT professionals must be proactive in all the areas mentioned above. Also develop, document and test all security procedures before putting them into production. Maintaining security is just as important as making it secure in the first place. You are either part of the solution or part of the problem.

Conclusion

Keep it secure by employing a system to prevent a security incident, detect a security incident and recover from a security incident. Recovery is the most important of the three. However each must be deploy and systematic used to provide the proper amount of security for your organization. Once the baseline of security standard are established, delegation of responsibility and function of each employee. Document all policies and ensure they are read. Document each procedure. Conduct a legal review of all policies and procedures. Document roles and responsibilities of each employee. Employees are the most important aspect of security. In most cases they are the first, second and last line of defense. So hire the best, the most honest and then educate them well. A security awareness program must become apart of the organization's culture. Keep it simple. Simple mechanisms tend to have fewer flaws to exploit and require less maintenance. Simplicity also helps in updating, replacing any mechanism because it is easy, straightforward and generally done quickly. Also strive of operational simplicity. Design a security system to allow for regular and easy adoption of new technology. As mission changes security must be updated. Constant security re-evaluation and correction, maintains security at a level that is dictated by management. As security threats change

so to must systems adapt to these changes. Funding is always an issue. When it comes to security is it like this, pay now or pay 10 times to 100 times more later or over the years doing security haphazardly. After a serious incident is no time to start to be concern about security. For future perseverance security must be address today and every day.

Reference:

Terry Wimsatt. "Recruiting for your Computer Security Vacancy" January 29, 2001.
URL: http://www.sans.org/infosecFAQ/securitybasics/recruiting.htm

Frederick Kim. "Information Security 101: Security for Newbies" 18 August 2001.
URL: http://www.sans.org/infosecFAQ/securitybasics/infosec_101.htm

Carnegie Mellon University. "CERT® Home Network Security". 2001
URL: http://www.cert.org/tech_tips/home_networks.html

Bundesamt für Sicherheit. "IT Baseline Protection Manual" July 2001.
URL: http://secinf.net/info/misc/gshb/etc/inhalt.htm

Sean Boran. "IT Security Cookbook" 06 September 2001
URL: http://www.boran.**com**/security/