Global Information Assurance Certification Paper

Implementing a Computer Security Compliance Program: Securing Your Network Enterprise from Known Vulnerabilities

Joseph Guntz Jr.

September 8, 2000

According to an article found at the SANS Institute web site, "a majority of successful attacks on computer systems via the Internet can be traced to exploitation of one of a small number of security flaws."[(1)] Although there are numerous resources available to publicize these vulnerabilities, I feel the lack of an organized process to track corrective actions taken to secure systems contributes to the problem of system compromises.

In order to ensure systems are secured against known vulnerabilities, I would suggest implementing a program designed to track actions taken to protect your systems from all identified vulnerabilities that apply to your network. I call this program the Computer Security Compliance Program (CSCP). The Air Force and other government agencies have similar programs in place but on a much larger scale. The goal of this program is to put in place, an organized process to document actions taken to secure an enterprise from known vulnerabilities that affect the systems under your control. The four steps that make up this program include notification, fix actions, testing, and documentation. Implementing this process will provide the network manager with a means to monitor the status of network security as it pertains to known vulnerabilities.

Notification is the first step to implementing the CSCP. It is necessary to stay current with the ever-changing environment of computer security as new vulnerabilities seem to constantly pop up. A visit to the Computer Emergency Response Team (CERT) web site shows that they have published 18 advisories from 01 January to 24 August 2000. [(2)] I have found many available resources that provide current and accurate information concerning vulnerabilities.

The best way to stay current is to join a few of the mailing lists that are available in the industry. These mailing lists provide the fastest means of notification and require the least effort for gathering this information. I suggest signing up for at least two mailing lists so that you can compare information that is being published. It can be thought of as getting a second opinion or a system of checks and balances.

Some of the mailing lists that I have found to be very helpful include the Microsoft Security Notification Service, the CERT Advisory Mailing List, and the BugTraq Mailing List. The three mailing lists above provide "alert" type notification. In other words, once they decide to publish information concerning a new vulnerability, an "alert" e-mail is sent to provide immediate notification. This service will allow faster reaction times so administrators can start the process of researching the vulnerability and reacting if necessary. Other highly recommended mailing lists include the SANS Security Alert Consensus and the Security Focus newsletter (SF-News). These weekly newsletters provide in-depth coverage of new vulnerabilities announced during the week.

Mailing lists are not the only means of finding out about vulnerabilities. Many computer security vendor web sites and e-zines have also proven to be excellent sources of information. For these resources to be effective, it is necessary to periodically visit these sites so that you can review updates. I would suggest visiting at least every other day to scan for breaking news. Computer security is a fast paced environment so a daily visit would not hurt. Some of the web sites that I find to be very helpful include:

SANS Institute: http://www.sans.org/newlook/home.htm
A cooperative education and research organization

Microsoft Security web page: http://www.microsoft.com/technet/security/
Location to find security bulletins put out by Microsoft

Computer Emergency Response Team: http://www.cert.org/
The CERT Coordination Center (CERT/CC)

Security Focus: http://securityfocus.com
Computer Security e-zine covering all facets of the industry

There are many other reputable mailing lists and web sites that provide the timely and accurate information that is needed to carry out the first step of the Computer Security Compliance Program. When documenting the standard operating procedures for your program, include the information resources that will serve as the authoritative source for notification for your organization.

The next step in the CSCP process is identified as "Fix actions". Once we have been notified about vulnerabilities that affect our enterprise, we must decide the best course of action to take. I like to break this process down into two parts. The first step is to review the recommended response to the identified vulnerability. Then we must evaluate how it may effect the affected system(s). Although I don't have a lot of technical experience with the intricacies of network administration, I do know that there should be a process in place to evaluate configuration changes (patches, changes to services allowed, etc.) prior to implementing these changes across the enterprise. Ensuring this evaluation takes place is part of the management process.

The next step is to implement the fix action on ALL affected systems. If the recommended action cannot be implemented due to its effect on the enterprise, this fact should be documented. If at all possible, an alternate solution should be implemented if one is available. Although documentation is the last step in the CSCP process, documentation in this instance refers to administrators letting it be known to all whom may be working the vulnerability, that they should not employ the recommended fix due to the expected adverse effects on the system. This documentation (notice) serves as a safety switch to keep everyone working the problem on the same "sheet of music".

Information pertaining to recommended fix actions is normally addressed in the vulnerability notification. If a fix action has not been identified at the time of the release of the notification, a follow up notice is usually released when a fix action becomes available. If alternate solutions are available to secure a vulnerability, you can normally find this information in the notification.

Now that the patch has been installed or configuration changes have been made, it is time to test the effectiveness of these changes. The third step in the CSCP process is the testing phase. A system that was once vulnerable to the latest hacker discovery must be considered still vulnerable until proven otherwise. I call this safe computing. The testing of a patched or fixed system is the confirmation required to ensure the fix actions where deployed and that they had the desired effect of securing your system.

Performing a penetration test against the recently identified vulnerability is one way to assess the results of implementing the fix actions. If the system can still be penetrated through the "patched" vulnerability, it is time to re-evaluate the actions taken. Review the initial notification for applicability to your system. Double-check the documented actions taken against the notification to ensure all required actions were accomplished. You can normally contact the source location of the notification if the work checked out but the patch didn't work. Nowadays, help is only an e-mail away. Be careful not to broadcast your open system vulnerabilities across the network. You can be sure there are people listening. Use of encrypted e-mail is a good solution to that problem.

Now that we have tested the system to ensure it is now secure from attack via the latest vulnerability, it is time to document our actions. This documentation will be the source of information that confirms the actions taken to secure the enterprise. The network manager and security administrators will be able to keep track of all measures taken to keep the enterprise secure and have a ready reference to review these actions. This documentation should include the vulnerability, date of notification, required action, administrator implementing fix, date system was patched (fixed) and tested, and supervisor's confirmation of actions. This may seem like a lot of information but the history created by this documentation could prove to be an invaluable tool should the system become compromised. This documentation will allow management to see the actions required to maintain a secure system. Having documented proof of the steps taken to secure the organizations enterprise may help to gain their support in time of crisis.

Now would be a good time to implement this program at any organization that has not taken steps to ensure their systems are protected from known vulnerabilities. The article found on the SANS web site, "How to Eliminate the Ten Most Critical Internet Security Threats"[(1)] would be the perfect starting point. In an article published in e-Week entitled "Securing dot-com", e-week labs recommends that organizations run security scanners on their networks to find vulnerable software. [(3)] Performing vulnerability assessments initially and then periodically will help to detect vulnerabilities that exist on your enterprise. Implementing the Computer Security Compliance Program will allow an organization to track the actions taken to patch known vulnerabilities. Any known vulnerabilities that can't be secured can at least be identified, documented, and monitored for intrusion. With the Computer Security Compliance Program in place, it should be easier to manage the security of your enterprise.

References:

1. The Experts' Consensus. "How to Eliminate The Ten Most Critical Internet Security Threats". Version 1.10, June 1, 2000 URL: http://www.sans.org/newlook/home.htm
2. Computer Emergency Response Team (CERT), Coordination Center URL:

http://cert.org/advisories/index.htm
3. Dyck, Timothy. "Securing dot-com", e-Week (06/26/00), URL: http://zdnet.com/eweek/stories/general/0,11011,2593629,00.html

Mail Lists

Microsoft Security Notification Service: URL: http://www/microsoft.com/technet/security/notify.asp

CERT Advisory Mailing List URL: http://cert.org/contact/certmaillist.html

BugTraq URL: http://www.securityfocus.com/frames/?content=/about/feedback/subscribe-bugtraq.html

SANS Security Alert Consensus URL: http://www.sans.org/newlook/digests/SAS.htm

Security Focus Newsletter URL: http://www.securityfocus.com/frames/?content=/about/feedback/subscribe-bugtraq.html

Vulnerability Assessment Information

INFOWAR.COM http://infowar.com/p_and_s/99/p_n_s_041799d_j.shtml