Guidance on Developing an Information System Patch Management Program to Address Software Vulnerabilities

Introduction

As financial institutions become increasingly dependent on commercial software to support critical business processes, they also increase their exposure to software vulnerabilities. Most financial institutions use multiple commercial software packages. Therefore, it can be challenging to identify, test, and install all of the applicable patches that are necessary to maintain each software package.

A patch management program should be part of an institution's overall computer security program. Oversight and accountability should be assigned to an appropriate party; however, the patch management program should include management, information security, and systems operations personnel. Consumer privacy regulations require that periodic risk assessments be provided to the Board of Directors.[1] In these assessments, management details measures taken to mitigate risks. The effectiveness of the institution's patch management program should be discussed in these periodic reports. An inadequate patch management program may adversely affect certain components of an institution's overall examination rating.

Risks of Inadequate Patch Management

Inadequate patching of software vulnerabilities exposes a financial institution to significant risk. Software vulnerabilities can cause system unavailability, create security weaknesses, and/or corrupt critical system components or data. Software vulnerabilities that result in security weaknesses can leave computer systems unprotected and open to access and criminal misuse of bank information by unauthorized parties, such as computer hackers.

Many computer viruses and worms are designed to exploit known system vulnerabilities. For example, viruses such as "Nimda," "Code Red," "I Love You," "Melissa," and the "Slammer Worm" all take advantage of system and security vulnerabilities to disrupt computer systems. In each of these cases, software patches are available from the vendor to eliminate the vulnerability, thereby neutralizing the virus. In the case of "Nimda," "Code Red," and the "Slammer Worm," software patches were available for a significant period of time prior to the widespread release of the virus.

[1] The credit union's patch management program should be discussed in its annual report to the Board of Directors pursuant to the NCUA Rules and Regulations Part 748, Appendix A, Section III(F), Guidelines for Safeguarding Member Information.

Developing an Effective Patch Management Program

An effective patch management program begins with appropriate organizational procedures, such as:

- Recognition of the risks posed by software vulnerabilities and direction for the implementation of a patch management program by senior management.

- Evaluation of current patch management processes to determine whether they are adequate as an ongoing patch management program.

- Documentation of the patch management program in policies and procedures. (In many cases, these policies and procedures may be incorporated into existing policies and procedures, such as the institution's information security policy or systems development and implementation policies.)

- Clear definition and assignment of responsibilities for patch management at a functional level, including prompt identification of vulnerabilities and relevant patches, evaluation and testing of the patches, timely implementation of patches appropriate to the environment, and tracking of both implemented and rejected patches.

- Documentation of decisions to install or reject specific patches.

- Audits, which can provide independent assurance that vulnerabilities have been identified and appropriate patches have been installed.

Additional procedures may also be warranted depending on the unique needs of the organization.

In developing an effective patch management program, it is important to have a comprehensive understanding of the institution's Information Technology (IT) environment. An up-to-date inventory of hardware and software should be maintained, including the specific applications and their location. At a minimum, it is suggested that the inventory include a description of the system's hardware, main frame and mid-range computers, operating systems (versions and all patches installed), application software (versions and all patches installed), and storage devices. This inventory should reflect production servers, firewalls, network appliances, routers, and other network several times a day or as seldom as once a year. The quality of vendor code may also influence patch frequency. Relevant patch information can be identified by subscribing to or reviewing the following sources of patch information:

- Vendor web sites;
- Vendor patch alert e-mail list subscriptions;
- Third-party security vendor web sites and e-mail alert services (these services may be fee-based);
- Third-party subscription or periodic vulnerability scanning and reporting services;
- Third-party public service security web sites and e-mail alert services (e.g., http://icat.nist.gov/icat.cfm, http://www.mitre.org/, and http://www.cert.org); and
- Internet discussion news groups related to patch management.

Evaluating the Impact of Patches

After a patch has been identified, an impact assessment of the application of the patch should be performed on the institution's information system and business environment, including a technical evaluation, a business impact assessment, and a security evaluation.

- *The technical evaluation* assesses whether the patch will correct a problem with the services and features of the application that are being used by the institution.
- *The business impact assessment* determines if applying the patch, or not applying the patch, will impact business processes and when may be an appropriate time for patch installation (i.e., immediately, after hours, or over the weekend).
- *The security evaluation* determines whether there are security implications that were not identified during the technical evaluation. Even though there may be no performance benefit to applying a patch, there may be security benefits. Patches may also be installed on software that may be loaded on a system but is currently inactive.

Institutions that maintain their own internal computer networks, but utilize vendor supplied financial applications, may be reluctant to install patches to their operating system until the financial application vendor has assured them that the operating system patch will not interfere with the financial application software. Institutions should work closely with their vendors to ensure that new patches are evaluated as soon as possible.

Testing and Installing Software Patches

Each patch should be tested prior to installation to ensure that it will function as expected and be compatible with other systems. Patches should be tested at a system level as well as in a quality assurance environment prior to their installation in the production environment. This will ensure their compatibility with the system and with other components in the environment. Evaluation and testing should also ensure that the installation of a patch or software update does not open vulnerabilities previously corrected or produce new vulnerabilities. Application of patches in the production environment is subject to normal change management procedures to minimize the risk of disruption due to installation of the patch. Testing should also occur in the production environment after installation.

In some cases, systems may need to be shut down to test and install a patch, which makes the system unavailable for a period of time. In the case where multiple patches may need to be installed, care should be taken to ensure that they are installed in the proper order. Otherwise, the patches may not be effective or cause additional problems.

If an institution reinstalls software, previously installed patches may need to be reinstalled (in the original order) in order to be effective. The original install media for the reinstalled software (e.g., CD-ROM, tape, floppy disk) should be maintained as well as all subsequent patches that were installed in the production environment. To simplify the reinstallation process, the institution can maintain current and previous system version backups of all software. Those versions can then be used in lieu of installing the software from the original installation media. An accurate inventory of systems and patch levels is essential in ensuring the recovery process is comprehensive.

Conclusion

Financial institutions may learn of computer software vulnerabilities from several sources. These include the software vendor, security vendors, subscription alert services, other users, and hackers attempting to gain unauthorized access to a system. Effective patch management will assist financial institution management in mitigating the risks associated with software vulnerabilities and in ensuring that the security and availability of computer systems are not compromised.