June 2016

What's in Your Third-Party Application Software?

Recently, it has been reported that third-party application software security vulnerabilities are on the rise. Third-party application software is designed to work within operating systems and to assist users in executing tasks on computers and other devices. For example, Microsoft Windows 7 is an operating system that controls the way computers work and how other programs function, but Acrobat Adobe is a third-party application that is utilized by computer users to create, modify, and read PDF files. Many Covered Entities and Business Associates may think their computers and devices that utilize operating systems are secure because the Covered Entities and Business Associates are deploying operating-system updates, but many systems are still at risk from third-party software.

According to a recent study, a majority of companies use third-party applications or software, but less than 1 in 5 companies has performed verification on these third-party software. Also, it was reported in companies that install their operating-system patches, a fair amount have third-party software that remain unpatched.

Furthermore, third-party software may have numerous security vulnerabilities that do not stem from the applications themselves. Misconfigured servers, improper files settings, and outdated software versions may contribute to third-party software security vulnerabilities.

Covered Entities and Business Associates Should Consider:

Testing Software Prior to Installation

Covered Entities and Business Associates should define the criteria they are willing to accept for safe third-party applications, including open source and public domain applications. Applications should meet the corporate standards set by the entities and also satisfy compliance requirements, and entities should test against these criteria.

The purpose of conducting security testing on software is to reveal flaws in its security mechanisms and finding the vulnerabilities or weakness of software applications. For example, conducting testing may find out how vulnerable a system may be to flaws in applications and determine whether data and resources are protected from potential intruders.

Covered Entities and Business Associates should work with their Business Associate vendors to test their applications for security vulnerabilities prior to installation, and on a regular basis after the software has been installed.

Installing Software Patches or Updated Versions

Software patches repair "bugs" in applications and software programs. Patches are updates that fix a particular problem or vulnerability within a program. Covered Entities and Business Associates should be installing patches or updating the software versions promptly and on a continuous basis. The majority of software developers disclose their security flaws to public; however, attackers exploit these known vulnerabilities if Covered Entities and Business Associates do not fix the security flaws in a timely manner.

Though applying patches is essential to ensure the security of information systems, patches should be assessed prior to deployment to determine the risk they pose to the Covered Entity's information systems.

Reviewing Software License Agreements

A software license agreement (also known as end user license agreement (EULA)) highlights the risks that can make ePHI vulnerable. Data can be compromised if Covered Entities and Business Associates ignore the language in a software license agreement, as such behavior can expose a computer and its connected networks and systems to security risks.

Software license agreements are legal binding agreements that can have restrictions on how the software can be used; the agreements can require entities to agree to certain conditions when using the software, and can also limit their ability to sue for damages.

To protect information systems and networks from security and privacy problems related to EULAs, US-CERT recommends that entities:

1. **Review the Software EULA** - Before installing any software, take the time to read its EULA.

2. **Beware of Firewall Prompts When Installing Software** – During installation, if your firewall generates a prompt asking whether you want to allow certain inbound or outbound connections, proceed with caution. Verify that the software requires changes to your firewall settings for normal operation and that you are comfortable with this operation.

3. **Consider the Software Publisher** – If you are not familiar with the company or organization that published the software, review the software EULA with added scrutiny.

Resources:

United States Computer Emergency Readiness Team (US-CERT): www.us-cert.gov - *(Software guidance)*