Developing a Patch Management Process

By Mike Bechtel, information security analyst, Vizo Financial

Everyone has a favorite pair of jeans they just can't part with, even after they've formed a hole or two. Not to worry, though, as you can easily patch the hole and repair the jeans.

The same can be said of your software and network. Cybercriminals and hackers are always looking for vulnerabilities within applications. In order to combat security threats, software companies release patches to fix the vulnerabilities. A patch can be applied to create a consistent, secure environment.

And just to be clear, EVERY kind of software needs to be patched at some point or another. Even the biggest and most reliable software companies offer patches for their products. In 2016 alone, Microsoft released 150+ security patches and Adobe released 10.

If your credit union doesn't apply these patches to your systems, you might be setting the organization up for exploitation in the form of malware, ransomware and more. These threats can take advantage of flaws in your software and applications in order to infect your computer systems, or even go so far as to hold all of your data hostage until you pay a fee.

The best way to prevent malicious threats from entering your systems is to develop a patch management process. The patch management process will guide you and your staff through patching your computers and systems. The process should include:

1. **Asset inventory.** Know what computers you have and what software and applications are installed so you can properly patch your network.
2. **Patch management officer or team.** A person or group of people should be designated to prioritize and stay up to date on the latest patches, as well as coordinate and implement patches.
3. **Timetables.** Patches should be assigned specific timeframes and schedules based on their priority.
4. **Deployment of patches.** This could be an automatic or manual process.
5. **Testing.** Testing should be performed to confirm the patches are working properly to protect your systems.
6. **Compliance verification.** Obtain proof that patches are being applied and that all computers are receiving those patches.

For more information on patches and upgrades, please contact the risk management team at riskmanagement@vfccu.org.

About Mike Bechtel

Mike Bechtel is an information security analyst for Vizo Financial. As such, he provides incident response planning services, information security risk assessments, security awareness training and information security-related consulting services to credit unions.