VOL. 5 | FEBRUARY 10, 2015

INFORMATION TECHNOLOGY UPDATE

Network Security: The What and How of Patching

Remember that day when you wanted to sneak out of the office five minutes early and instead had to stay a few minutes late because your computer needed to install 16 updates before shutdown? That (often bothersome) update is an example of a "patch," or piece of code developed to correct problems or assist added functionality. Even if you're not an IT wizard, you can presume that countess patches are necessary to ensure a safeguarded, functional network. Despite the severe need to install patches, IT staff mistakenly omit them due to their complex, progressive nature.

The Open Web Application Security Project's Top 10 Security Risks listing for organizations includes five frequent vulnerabilities that can be mended through patching (2010). If missing patches increase an entity's susceptibility to an attack, why do IT staff overlook patches, and what can you do to make sure your institution is executing effective patch management?

What Do I Need to Patch?

There are only two groups of items that need to be patched: (1) software packages and (2) the operating system. Staff typically neglect the first group in terms of successful patch management. Here are a few reasons why:

- Many of the automated patching systems only secure the operating system itself and not the software on the operating system;
- IT staff simply don't realize that there are patches available or do not think that the software in question could lead to a compromise;
- Staff neglect to reboot the system after implementing a patch. This provides a false sense of security because the patch is not effective until after the reboot. Hacker tools will tell an intruder how long it has been since a system reboot and what patches were partially installed; and
- Users install unauthorized software. The IT staff are unaware of the software's installation and its missing patches.

Regardless of the above reasons for an unpatched software package, a single, neglected patch can lead to the compromise of numerous hosts on the network. Although all software packages should be monitored, banks should pay closer attention to certain types.

Typically, larger software vendors require extra patches. For example, Microsoft (as an operating system) has more patches than a small banking application. To explain, the source code for the banking application is harder for hackers to come by than exploits in the Windows code. In other words, Microsoft and other operating systems are threatening targets to institutions because they're common, readily available, found on most internal computers and servers, and less expensive compared to small banking applications.

2100 Corporate Drive, Suite 400 Wexford, PA 15090 | Phone (724) 934-0344 | Fax (724) 934-0345 | Email: info@srsnodgrass.com
1275 Glenlivet Drive, Suite 135 Allentown, PA 18106 | Phone (610) 530-8885 | Fax (610) 530-0409
2100 Renaissance Blvd., Suite 110 King of Prussia, PA 19406 | Phone (610) 278-9800

How to Employ Effective Patch Management

Now that you know what needs to be patched, how can you effectively employ patch management at your bank? Exercising patch management will involve one of two methods—patching systems manually or by using an automated software package—or a combination of the two. IT staff can purchase automated software packages that patch the operating system and software loaded. This method is useful for large institutions since manually locating and installing absent patches takes a considerable amount of time. Be forewarned that none of these software packages are 100 percent guaranteed to catch all needed patches. Therefore, IT staff need to be diligent at looking for software that these automated systems may be unable to patch.

Smaller institutions with fewer network systems may attempt the time-consuming manual approach instead of the pricier automated method. Both solutions require one piece of documentation that many bank personnel, auditors, and regulators overlook: a detailed software inventory. A well-kept software inventory, whether compiled manually or derived from an automated software program, should list all installed software on every machine in the organization. With this inventory, the IT staff can check software vendor websites for needed patches and possibly discover unauthorized software loaded by end-users that can be removed.

To determine if your organization is building its best barrier for attacks, IT staff should schedule regular penetration tests (from both an external and an internal perspective), as many of the software tools used during a penetration test can search for missing patches and misconfigurations. A well-conducted penetration test can be the proof that examiners or regulators, audit committees, and senior management of the bank need in order to assure the organization that the patching system in place is working as designed. Vulnerabilities discovered should be quickly remediated, but more importantly, patching processes should be adjusted to certify the same type of susceptibility is not rediscovered in the future.

In Summary

IT staff should regularly visit software vendor and operating system websites (regardless of the patching system in place) to search for patches for security-related issues. In addition, IT staff should maintain a detailed software inventory to validate patches and perform periodic reviews of user workstations. Missing patches should be installed as soon as possible and during non-peak hours so the system can be rebooted. Automated patching systems, while often robust and helpful, should not be fully relied upon to patch the entire network. Lastly, regular penetration tests should be conducted to make sure the patching system in place is operating as intended.

Remember, a single missing patch or misconfiguration of software can lead to the compromise of your entire network. Don’t give an attacker a "foothold" to start climbing into your network.

References

The Open Web Application Security Project. 2010. Top l0 2010 - Main: Top 10 risks. Retrieved January 30, 2013 from https://wwwowasp.org/index.php/Top-10-2010-Main.

Questions?

If you wish to discuss any of the above items, please contact Jeremy Burris or Rob Haller at (724) 934-0344, or email at jburris@srsnodgrass.com or rhaller@srsnodgrass.com.