OUCH! I May 2020

SANS SECURITY AWARENESS

OUCH!

The Monthly Security Awareness Newsletter for you

The Power of Updating

Overview

You may not realize it but cyber attackers are constantly looking for and finding new vulnerabilities and weaknesses in the software people use every day. This software may run your laptop, could be the mobile apps you use on your smartphone, or perhaps even the software in your baby monitor or other devices in your home. Bad guys take advantage of these software weaknesses, allowing them to remotely break into devices around the world. At the same time, the software and device vendors are constantly developing fixes for these weaknesses and pushing fixes out as software updates. One of the best ways you can protect yourself is to ensure the technologies you use all have the latest updates, making it much harder for cyber attackers to break into them.

How Updating Works

When a software vulnerability is discovered, a software update (also known as a patch) is developed and released by the vendor. Most software programs and devices nowadays have a mechanism to connect over the Internet to a vendor's server to obtain the software update. This update, nothing more than a small program, typically installs itself and fixes the vulnerability. Examples of software you need to update are the operating systems that run your laptop (such as Microsoft Windows or OSX) or run your smartphone (such as Android or iOS). Additionally, but often overlooked, you need to update the programs that run on your devices, such as your laptop's web browser, word processor, messaging software or your phone's mobile apps (especially social media apps).

This is why, whenever you purchase a new computer program or a new mobile app, check first to be sure the software vendor is actively updating the program or device. The longer software goes without any updates, the more likely it has vulnerabilities that cyber criminals can exploit. This is why many vendors, such as Microsoft, automatically release new patches at least every single month.

Finally, if you are no longer using a certain computer program, software or mobile app, remove it from your system. The less software you have to update, the more secure you are.

Updating

There are two general ways of updating a system:

Automatic - Whenever a device, operating system, program, or mobile app detects that a new update has been released by the vendor, it automatically downloads and installs the update. The advantage of automatic updates is that you don't have to do anything. The software ensures that the technologies you are using are current. The disadvantage of automatic updates is the updated program could cause a problem resulting in the loss of functionality or data. This is rare for personal devices, but can happen for more complex environments, like large corporations.

Manual - When an update for a device, operating system, program, or mobile app is available, you must manually download and install the update. This gives you more control over what and when updates are installed. Larger organizations (such as hospitals or utilities) typically like manual updates because it allows them to test the changes first to detect and address any issues caused by the update. The disadvantage of manual updates is that it may take you much longer to update the system, or you may even forget to install the update.

Conclusion

For individuals, families, and small businesses, we highly recommend you enable and use automatic updating on all of your devices. This ensures that all of the technologies you are using, from your smartphone and laptop to your baby monitor and door locks, all have the latest software. Up-to-date devices and software make it that much harder for any bad guys to attack them. Enabling automatic updates is one of the simplest and most effective ways to protect yourself and securely make the most of today's technology.

Guest Editor

Don C. Weber is an information security leader with extensive experience in DFIR, pentesting, research, and management since 2002. Don has participated in the SANS Advisory Board, Ethics Committee, Gold Program, and is currently an instructor for ICS410. Don can be reached at @cutaway and https://www.cutawaysecurity.com.

Resources

Got Backups https://www.sans.org/security-awareness-training/resources/got-backups

Four Simple Steps to Being Secure
https://www.sans.org/security-awareness-training/resources/four-simple-steps-staying-secure