The importance of updates

At some point in time, you may have wondered, “Why do my devices constantly need updating?” For consumers, updates provide improvements to performance, stability, and even new features! But from a security standpoint, they serve a specific purpose. Updates allow organizations to address security vulnerabilities that can place their users, devices, and networks at risk.

In a video, you learned that updates fit into every security team’s remediation strategy. They usually take place after a **vulnerability assessment**, which is the internal review process of an organization's security systems. In this reading, you’ll learn what updates do, how they’re delivered, and why they’re important to cybersecurity.

Patching gaps in security

An outdated computer is a lot like a house with unlocked doors. Malicious actors use these gaps in security the same way, to gain unauthorized access. Software updates are similar to locking the doors to keep them out.

A **patch update** is a software and operating system update that addresses security vulnerabilities within a program or product. Patches usually contain bug fixes that address common security vulnerabilities and exposures.

Note: Ideally, patches address common vulnerabilities and exposures before malicious hackers find them. However, patches are sometimes developed as a result of a **zero-day**, which is an exploit that was previously unknown.

Common update strategies

When software updates become available, clients and users have two installation options:

- Manual updates
- Automatic updates

As you’ll learn, each strategy has both benefits and disadvantages.

Manual updates

A manual deployment strategy relies on IT departments or users obtaining updates from the developers. Home office or small business environments might require you to find, download, and

install updates yourself. In enterprise settings, the process is usually handled with a configuration management tool. These tools offer a range of options to deploy updates, like to all clients on your network or a select group of users.

Advantage: An advantage of manual update deployment strategies is control. That can be useful if software updates are not thoroughly tested by developers, leading to instability issues.

Disadvantage: A drawback to manual update deployments is that critical updates can be forgotten or disregarded entirely.

Automatic updates

An automatic deployment strategy takes the opposite approach. With this option, finding, downloading, and installing updates can be done by the system or application.

Pro tip: The Cybersecurity and Infrastructure Security Agency (CISA) recommends using automatic options whenever they’re available.

Certain permissions need to be enabled by users or IT groups before updates can be installed, or pushed, when they're available. It is up to the developers to adequately test their patches before release.

Advantage: An advantage to automatic updates is that the deployment process is simplified. It also keeps systems and software current with the latest, critical patches.

Disadvantage: A drawback to automatic updates is that instability issues can occur if the patches were not thoroughly tested by the vendor. This can result in performance problems and a poor user experience.

End-of-life software

Sometimes updates are not available for a certain type of software known as end-of-life (EOL) software. All software has a lifecycle. It begins when it’s produced and ends when a newer version is released. At that point, developers must allocate resources to the newer versions, which leads to EOL software. While the older software is still useful, the manufacturer no longer supports it.

Note: Patches and updates are very different from upgrades. *Upgrades* refer to completely new versions of hardware or software that can be purchased.

CISA recommends discontinuing the use of EOL software because it poses an unfixable risk to systems. But, this recommendation is not always followed. Replacing EOL technology can be costly for businesses and individual users.

The risks that EOL software presents continues to grow as more connected devices enter the marketplace. For example, there are billions of Internet of Things (IoT) devices, like smart light bulbs, connected to home and work networks. In some business settings, all an attacker needs is a single unpatched device to gain access to the network and cause problems.

Key takeaways

Updating software and patching vulnerabilities is an important practice that everyone should participate in. Unfortunately, that’s not always the case. Many of the biggest cyber attacks in the world might have been prevented if systems were kept updated. One example is the WannaCry attack of 2017. The attack affected computers in more than 150 countries and caused an estimated $4 billion dollars in damages. Researchers have since found that WannaCry could have been prevented if the infected systems were up-to-date with a security patch that was made available months before the attack. Keeping software updated requires effort. However, the benefits they provide make them worthwhile.

Revision #1
Created 20 August 2023 08:10:19 by naruzkurai
Updated 20 August 2023 08:24:13 by naruzkurai