PATCH MANAGEMENT

Did you know?

The average time to patch a vulnerability or **"MTTP" (mean time to patch) is between 60 and 150 days.**[1] Meanwhile, the average exploitation is most likely to occur within the first month following the initial patch.[2]

What is patch management?

Patch management is the practice of deploying software updates to your environment to keep it operating efficiently and, most importantly, capable of repelling common cyber threats.

Why is this important?

Patch management is a critical component to secure systems. The technology sector moves at a rapid pace. This is true for both its key corporate players as well as the malicious actors who exploit it. The newest and greatest software will always have bugs to be fixed or enhancements to be made. More gravely, it will always be subject to new vulnerabilities.

What are vulnerabilities?

A vulnerability is a security gap in a software that leaves a user vulnerable to exploitation. Cyber criminals are constantly reviewing source code to identify vulnerabilities. When they find them, our team inevitably sees a substantial influx of clients undergoing related attacks.

A vulnerability exploit is categorized as "zero-day" when attacks occur prior to a solution existing, because the creator has "zero days" to prepare a response for this unknown flaw. This is why timing matters. By the time patches are released, cyber criminals have already been working to exploit the vulnerability.

1. https://resources.infosecinstitute.com/topics/vulnerabilities/time-to-patch-vulnerabilities-exploited-in-under-five-minutes/#:~:text=Security%20metrics%20are%20a%20helpful,to%20push%20out%20a%20patch.
2. https://www.mandiant.com/resources/blog/time-to-exploit-trends-2021-2022#:~:text=Following%20public%20disclosure%20of%20a,exploited%20within%20a%20second%20week.

PATCH MANAGEMENT

What are the consequences?

Poor Performance

Technology by its nature is constantly evolving. Good patch management ensures everything is working to the best of its ability. Without it, you are inevitably limiting your efficiency.

Non-Compliance

Many industries are subject to regulations and guidelines that require certain security standards to be met. Prompt patching is a common inclusion. Failure to meet compliance requirements can be met with fines or other enforcement actions.

Cyber Attacks

Cyber criminals exploit vulnerabilities to gain access then unleash a variety of attacks within your environment. This often leads to ransomware attacks, where they shut down your operations and hold your data for ransom.

A study done by the Ponemon Institute found that existing patches could have prevented 57% of cyber attacks.[3]

How to maintain good patch management?

Be proactive. Create a procedure that prioritizes prompt and efficient patching, and make sure it is followed. You can usually find updates on vendor websites. Take caution that any updates are only downloaded from trusted vendor websites! Many vendors also offer automatic updates, which is an excellent way to stay up to date.

[3] https://www.cybertalk.org/2022/10/17/vulnerability-and-patch-management-trends-and-tips/#:~:text=A%20study%20conducted%20by%20the,prevented%2057%25%20of%20cyber%20attacks.