WEI INSIGHTS TECH BRIEF

THE CRITICAL IMPORTANCE OF PROACTIVE PATCHING AND UPDATES

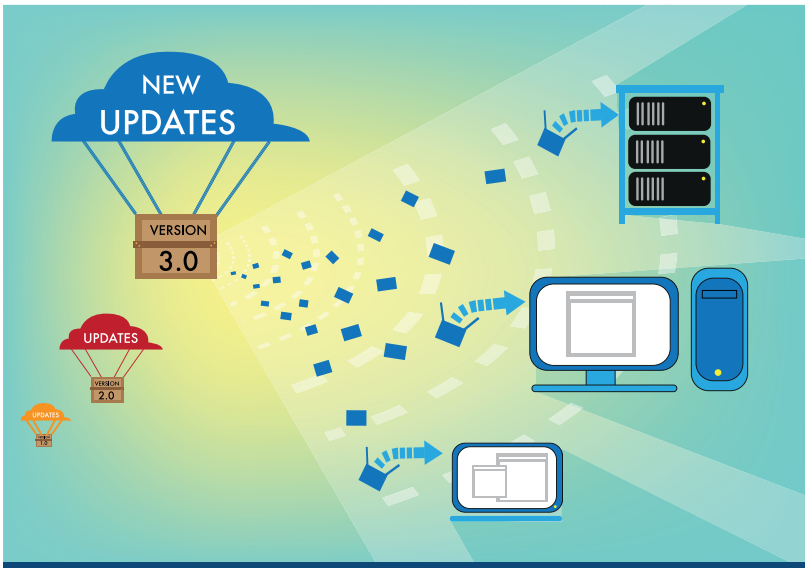
Businesses of all sizes must contend with a constant stream of patches and updates to keep their IT infrastructure operational and secure. Despite the vital importance of making proactive updates to software and firmware, few businesses are rigorously implementing the best practices to stay current with the latest versions of all the software and firmware in their network. Why are so many businesses failing at this critical task?

There are many reasons. The first is that there are often too many patches for IT staff to keep up with. While some companies like VMware release new patches only when necessary, others companies like Microsoft and Oracle patch on a regular cycle, meaning that patches can arrive before the last batch has been reviewed, let alone installed. This deluge can make patch management difficult in even the most organized, well-staffed IT departments.

Another reason we often see among our clients is complacency. Once a system is up and running, engineers are hesitant to rock the boat. Applying new patches and updates to a healthy network requires service interruptions, the introduction of instability, and allocating man-hours to a project that has little immediate benefit. In these cases, it's much easier to focus on higher-visibility projects and hope for the best in regards to patching.

The roadblocks to proactive patching and updating can be particularly daunting to larger organizations. In these scenarios, engineers must carefully ensure that the right patches are being correctly applied to each part of the network infrastructure, including the operating systems, network servers, routers, switches, firewalls, and mobile devices — as well as off-premises systems. These patches and upgrades must be reviewed and applied in a carefully determined order to prevent the disruption of network services, further complicating the task. While some organizations have dedicated patch administrators to handle these tasks, many do not.

Despite these challenges, there are some vitally important reasons to stay current with the latest software and firmware updates, and severe consequences await companies that fail to do so.



Despite the vital importance of making proactive updates to software and firmware, few businesses are rigorously implementing the best practices to stay current with the latest versions of all the software and firmware in their network.

WEI

DANGER TO YOUR BUSINESS

The most urgent of these reasons is that outdated systems are an easy target for viruses and malware. In recent years, attacks by spyware, ransomware, rootkits, hijackers, and other types of malware have continued to do an increasing amount of damage to enterprise networks, causing decreased productivity and lost revenue. Many of the highest-profile breaches in recent history have all been directly attributable to poor patching.

Take for example Equifax, the largest data breach in recent years. Hackers entered Equifax's network through a vulnerability in the Apache Struts web application in May of 2017, a vulnerability that had been identified and patched two months earlier, in March of the same year. Failing to stay current with their patching efforts led to disaster for Equifax, costing the company over $4 billion dollars and leaking the personal information of over 145 million people.

The NotPetya outbreak is a similar story, as it exploited the same vulnerability that the WannaCry attack had exploited—even though the vulnerability had been patched already. In this case there were enough unpatched computers for malware to spread and wreak havoc, shutting down the radiation monitoring system at Chernobyl's Nuclear Power Plant, dealing $300 million dollars in damage to shipping firms Fedex and Maersk, and destroying the computer networks at multiple hospitals.

Despite the motivation that these high-profile cases provide, a vast majority of businesses are failing to do the work required to stop these highly-destructive types of malware. According to a poll of 318 organizations by research firm Voke Media, 80% of the companies that either had a data breach or failed a security audit could have prevented the problem with more vigilant software patching or configuration changes.

AVOID MAJOR DOWNTIME OR SERVICE DISRUPTIONS

Ensuring that your systems continue to operate smoothly as they scale out and add new services is another important reason to stay vigilant with patches and updates. Network upgrades can be a long and complex process that involves months of careful analysis and preparation. Discovering at the last minute that a planned upgrade will cause incompatibilities with an existing service can derail that carefully coordinated effort, delaying the deployment of critical new services and wasting time and money.

The problem of incompatibility can even be a factor when tapping new functionality in existing applications or network equipment. Simply because an appliance or piece of software has a certain function, doesn't always mean that the function will turn on like a switch when needed. When bringing new services online, it's important to make sure that all hardware and software has been patched and upgraded in such a way that these services will interwork smoothly with the existing infrastructure. This is especially true in large or complex network environments, or in those running customized or proprietary software applications.

ORGANIZED AND PROACTIVE PATCH MANAGEMENT IS THE ONLY SOLUTION

It's clear that proactive patch management is vital to the health of your enterprise, but what does that strategy include? The first step in developing this strategy is to evaluate your organization's network and systems to gauge their overall health. Without a healthy IT system to provide a foundation for your patch and update management strategy, this strategy runs the risk of being either incomplete or ineffective. Once your systems have been stabilized, your in-house IT staff or technology services provider should begin to devise a patch strategy that includes the following components.

- **Prioritize key applications**
  It's unrealistic to expect to apply every single patch or update to your systems at once, for the abovementioned reason that they're released at an unmanageably fast pace. Because of this, it's critical to have a clear picture of which parts of your network are most vulnerable, and to prioritize them in your patch management strategy.
- **Collect and evaluate patches**
  Organizations should have a dedicated staff member or team to collect information about all the new patches and updates that pertain to your network. During this process, they should also determine which patches and updates need urgent attention, and which ones can wait.
- **Patch testing**
  In a perfect world, all critical patches would be tested in a test environment that closely resembles the production environment. After verifying the digital signature or integrity of the patch, testing should ensure that the system reboots without error and that key applications can run trouble-free. For mission-critical systems, this testing could be expanded to include the execution of scripts or other programs to ensure full application functionality.
- **Patch Deployment**
  The final stage of the patch process is where the actual patch or update is applied. Patching clients can sometimes be done with tools that schedule the patches during off-peak hours to minimize service interruptions, while updating mission- or business-critical servers must be done manually in case implementation of a recovery plan is required.

SUSTAINED EFFORT IS CRITICAL TO PATCHING SUCCESS

Comprehensive patch management is a complex process that involves gathering and reviewing release notes, evaluating the changes and revisions in each update, and devising a systematic plan to ensure those changes are implemented safely. What makes patch management such a challenge for the majority of businesses is its relentless nature. It takes consistent effort and a high degree of organization to effectively manage the patches and updates in a secure and uniform fashion.

For this reason, many companies choose to outsource their patch management, as doing so frees your staff to concentrate on other, less onerous tasks. This can help them avoid "patch fatigue," a term coined by Tripwire to describe why so many IT professionals (67%) fail to stay consistent with their patching efforts. By outsourcing to a service provider, organizations not only avoid the problem of fatigue but also take advantage of the expertise and economies of scale that IT service providers possess. With the latest tools and a well-informed, big picture view of the overall landscape, IT service providers can streamline the process of staying current with patches and updates, often for a reasonable flat fee that is significantly cheaper than using in-house staff.

Whether they're done in-house or by an external partner, patch and update management is a crucial—though often overlooked—aspect of ensuring the long-term security and prosperity of your business.

WEI

TALK TO WEI TODAY

Talk to WEI today about our customized solutions to proactively manage the patches and updates in your network. We can help ensure that your operations remain at optimal security and efficiency with a lot less busy work on your behalf.

ABOUT WEI

WEI is an innovative, full service, customer centric IT solutions provider.

Why WEI? Because we care. *Because we go further.*

At WEI, we're passionate about solving your technology problems and helping you drive your desired business outcomes. We believe in challenging the status quo and thinking differently. There are a lot of companies that can take today's technology and create a great IT solution for you. But we do more. We go further. And we have the customer, vendor and industry awards to prove it. WEI is a premier technology partner, who always puts our customers first while providing the most innovative solutions for over 25 years.

WEI Dedication meets innovation.

info@wei.com
www.wei.com
43 Northwestern Drive | Salem, NH 03079
800.296.7837