Patching in a Hybrid Cloud World

How you can address four key patching challenges

Anthony Bryce, director of product management for BMC Digital Service Operations, discusses why patching still matters and how do it right in an era of complex, hybrid cloud infrastructures.

Anthony Bryce

DIRECTOR, PRODUCT MANAGEMENT, BMC DIGITAL SERVICE OPERATIONS

Anthony has 20 years of experience in the IT Service Management space working in a variety of roles from software consultant to solutions architect. For the last 10 years, he has been focused on product management and marketing, working on strategic projects, delivering detailed market analysis, and identifying new product opportunities and bringing them to market.

Do you think software patching is still important?

Patching will never be a glamorous, pulse-racing exercise, but it's absolutely essential to the safe and secure running of business services and applications. Too many organizations wind up in the news for the wrong reasons because they failed to effectively patch, and it led to a security breach or a critical business service outage.

What are some of the challenges organizations have with patching?

Many organizations run a broad array of operating systems and applications across in-house and cloud platforms, and it's not uncommon for each to use a different tool and approach for patching. Different vendors issue patches on different schedules using different mechanisms, which makes organizing and scheduling pretty challenging for the IT operation teams.

It also can be hard to prioritize patches because it's difficult to know which systems support which applications and business services. Business owners may also delay patches because they often involve downtime or the risk of application issues, but this in turn can increase other security-based risks.

The patch process itself involves much more than just deploying a file to a server or other device. For every new patch, the operations team must determine which IT components are affected, test them, gain approvals, and schedule updates that align with appropriate maintenance windows. Even the patch-approval process can be challenging, often involving a change manager and potentially dozens of business owners and other stakeholders.

Do you agree with some recommendations that, rather than patching, organizations should just update the underlying image and redeploy servers?

You really need to do both. For example, one of our customers said they can only update underlying images about every 8 weeks, potentially leaving servers vulnerable to attack for up to a 2 month period. In the end they agreed that they need to both update images and patch on a more regular basis. We also see organizations patching their public cloud infrastructures, but not taking the other vital step of updating the images from which they create new servers. This means they might re-provision the same vulnerabilities back into their environment. Its important to regularly identify vulnerabilities and close them down as well as update or create new and secure golden images.

What's next for patching as an IT operations discipline?

There are four basic challenges. The first is the variety of technologies to be patched. Second is prioritizing patches from a business perspective. Third is getting business stakeholders to buy into the importance of patching, and fourth is reducing the effort, cost, and time involved.

We're tackling all of these. Our core configurations tools provide very broad coverage across different operating systems, eliminating the need to use multiple tools. We're also putting patching into

Patching will never be a glamorous, pulse-racing exercise, but it's absolutely essential to the safe and secure running of business servicesand applications.

a business (rather than a technology) context by taking information from application discovery tools to better plan and execute complex patch processes. This allows the change manager to help coordinate patches to systems that affect a business service and schedule to predefined maintenance windows.

BMC is now able to leverage data from security scanning tools to understand the criticality of various vulnerabilities to help us prioritize risk-mitigation activities. This helps accelerate patching analysis and provides better visibility into the existing risks and the actions taken to address them.

We are also automating complex pre and post patch activities, like coordinating the shutdown and restart of interconnected systems as they are patched. Considerable efficiencies can be found through fully automating the patch process meaning less downtime and more successful outcomes. Consider a cancer hospital that is using our software to patch their patient care support systems. They have automated the entire process, from notifying nurses in the ICU to be on standby to removing systems from high-availability clusters, patching and then putting them back in the cluster. All of this is aimed at ensuring that patients' needs are met and that systems are current and protected from vulnerabilities.

As a final note, not all vulnerabilities are addressed through patching. Configuration management – things like making sure unneeded ports and services are disabled – is also essential for both security and compliance. That includes fine-grained control of who can make changes to systems, and tracking who made what changes and why. We helped an insurance company keep control of their server configurations by doing approximately 150 nightly checks of various configurations, including software versions, network settings, access rules, and more. If the desired configurations deviate from the desired state, they are notified, a change is recorded, and an auto-remediation action can occur. This greatly improved their server configuration, leading to better security and compliance at a very low administration cost.

What does success look like for an organization when it comes to patching? How do organizations move up the maturity curve?

One key metric is how much of your infrastructure has been properly patched. While most organizations achieve only 60 percent patch rates, leading organizations are able to achieve rates over 90 percent. One of our customers got to 99 percent through the combination of automation, understanding business context, and instilling patching as a top priority and holding the business more accountable. Some of our customers have seen patch rates soar by taking a "wall of shame" approach and circulating the names of business owners who fail to approve patches.

The second metric is how quickly you close server vulnerabilities. The industry average is 193 days, yet the first exploit happens, on average, only 30 days after the patch is released. This is a huge time gap that organizations need to close.

What are the two to three things for CIOs and information technology decision-makers to keep in mind when devising a software-patching strategy?

Start with a good inventory of all your operating systems and applications, in the public cloud as well as your internal data centers. You'll need patching and configuration management tools that cover all those platforms with consistent processes — ideally, built around not individual bits of technology, but the services that drive your business. That helps application owners understand how patches keep the business up, running, and secure, and helps the patching team streamline approvals and gain cost efficiencies.

Second, don't forget to automate the steps around the deployment of the patches, such as ingesting vulnerability scan data, discovering business system context, scheduling against maintenance windows, and integrating with change-ticketing systems. These ancillary steps can significantly slow processes and delay effectiveness.

Finally, make someone – ideally, a business owner – responsible for patching so it doesn't fall through the cracks and put your organization in the news for the wrong reason. ■