4 Steps to Patch Management Success

by Eric Vanderburg

The need for patch management

has repeatedly been demonstrated in recent years as companies large and small suffered data breaches due to unpatched vulnerabilities. The patch management function of applying patches to remediate known vulnerabilities may seem simple, but even one unpatched computer can lead to compromise. Last year the Equifax network was breached from an unpatched machine, resulting in the exposure of personal information from 143 million people. Patch management difficulties are faced by a wide range of companies too. The WannaCry ransomware exploited a known vulnerability in over 400,000 machines, resulting in millions of hours in lost employee time, loss of customer confidence, and loss of data. The patch for this vulnerability had been available for almost 60 days at the time of the attack.

The risks of failing to apply patches are clear, but it is important to point out that patch management is not as easy as it seems. Companies face real challenges in keeping a myriad of systems and applications current with the latest patches.

Patch management challenges

Patch management can be complicated as organizations extend into multiple sites and clouds on heterogeneous platforms. The modern enterprise consists of many systems and applications that may each have different patch release schedules. In addition to routine patch releases, vendors may also release critical patches to address urgent vulnerabilities. Many vendors are releasing patches on increasingly frequent schedules to more efficiently stay on top of newly discovered vulnerabilities, but this makes it more challenging to manage patch deployment. Rapid patch release schedules also require timely patch deployment strategies. Traditional patch deployment schedules are unable to meet the cybersecurity needs of today's swiftly changing environment.

These challenges are significant, but not overwhelming with these four steps:

- **Visibility**
- **Risk management**
- **Orchestration**
- **Validation**

Visibility

The starting point for any IT organization is to understand what needs to be patched. Visibility is needed across the enterprise, including heterogeneous server and cloud environments, to identify patch levels of each system and application as well as the available patches for these systems.

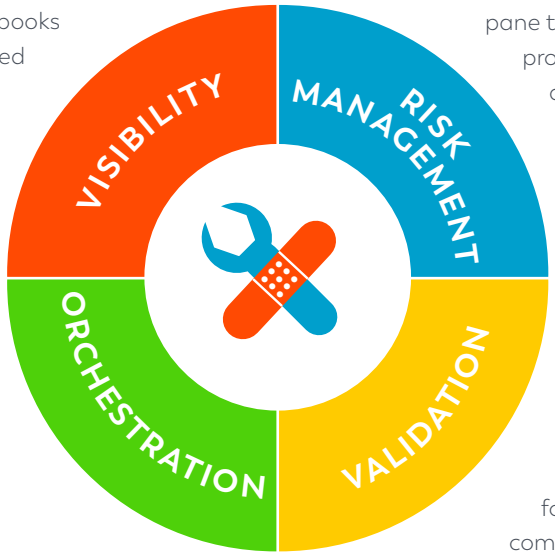
bmc IDG

Risk management

Next, organizations should manage risk by establishing a set of patch management risk metrics. These metrics reveal which software patches are most urgent and critical. The risks associated with each patch need to be identified and prioritized for management.

Orchestration

Orchestration is the next significant step in the process. Orchestration runbooks and workflows should be created to deploy patches while minimizing the impact on system availability. Orchestration is a vital cybersecurity component because it reduces the likelihood of human error. Even the most well-intentioned person can make a mistake once in a while, but a properly configured system will perform the task with the same level of diligence every time.



The first orchestration step is to validate the potential impact of deployment on system stability. This may involve simulation of patch deployment or deployment of patches to a test environment first. The second step is to deploy patches with minimal or no downtime to production systems. For example, the patch management process may need to pause cluster nodes or migrate applications from a node before patching and then migrate applications or nodes back after patches have been applied. Orchestration should be implemented according to organizational risk management policies so that patch deployment timeframes vary depending on patch risk metrics. For example, organizational policy may require that patches addressing a critical risk be deployed within four hours while medium risk items may be deployed on a weekly schedule.

Validation

The last step is to confirm that patches have been applied consistently to enterprise systems based on the policy. As demonstrated by Equifax, it is not enough to just apply patches; companies must also verify that deployment was successful. This ensures that systems do not slip through the cracks and provide a weak link for attackers. Even when cloud system patch management is managed by a cloud provider, or when IT services are outsourced, organizations must still be able to ensure that third parties are patching systems according to contractual agreements or established standard operating procedures.

Dashboards and alerts are very effective in the validation effort. Dashboards provide a single pane to view patch management progress and current status while alerts can keep responsible parties notified of important patch management actions.

Tools and Services

The four-step approach above requires a set of tools and services to implement and it is important to select a tool that fits into the overall technology management portfolio. Patch management is one component of overall system lifecycle management and some tools such as BladeLogic Server Automation by BMC can be used to manage this process in addition to other system lifecycle tasks. Combining patch management functionality with other system lifecycle management reduces the number of services that need to touch each system and the configuration effort required to integrate services. It also provides a single place to manage efforts and reduces overall management complexity

The importance of patch management cannot be understated. It is a critical component of any cybersecurity strategy and one that companies need to implement correctly to have confidence in their technology systems. A robust management system is needed to stay on top of system vulnerabilities and patch management risks.

Eric Vanderburg is a Christian cybersecurity leader, consultant, author, and thought leader. Vanderburg leads the cybersecurity consulting division at TCDI. Follow him on Twitter @evanderburg