Smart Patching for Smarter Security

How an automated approach can help state and local governments reduce vulnerabilities and improve efficiencies

In the first quarter of 2017 alone, nearly 5,000 software and server vulnerabilities were reported. Many were found in software that state and local governments rely on for daily operations.[1] To avoid the kinds of cyber attacks that create headaches and headlines, government organizations need to update devices, servers and other assets as soon as possible after a patch is released. If they don't, they risk exposing citizen data, losing critical services, and violating compliance with internal and external regulations. Although organizations can significantly reduce their attack surface by patching quickly, correctly and across all assets, doing so can be complicated, time consuming and error prone. By automating the patching process and following best practices, state and local governments can improve their security posture, save money and free up time to meet mission goals such as improving citizen service.

The Pitfalls of Patching

In an analysis of 600 local, state and federal government organizations' security posture, 90 percent of lower-performing state organizations scored an F in software patching cadence. Among local organizations, 50 percent of low performers received an F.[2] State and local governments face the following challenges related to patching:

Sophisticated attacks. Cyber attacks are increasingly stealthy and targeted, and government organizations are not immune. Destructive malware was used to wipe disks in both the Ukraine and Saudi Arabia recently — highlighting the fact that IT security is a national issue.[3] In many cases, even criminals who are not tech savvy can gain access to attack tools.

Vulnerabilities in legacy software. Government organizations often have legacy systems that are no longer supported by vendor software patches. These systems have been around for a long time, giving cyber criminals ample time to discover vulnerabilities. The recent WannaCry ransomware attack that hit hundreds of thousands of computers exploited known Microsoft Windows vulnerabilities and was so virulent that Microsoft made an exception and created a patch for computers it no longer supports.

Visibility. Many organizations have thousands of devices that need to be discovered, tracked and updated. Managing these assets, and the software running on them, is a challenge in today's complex environment of extended enterprises, virtual machines, traditional (physical) software solutions and disparate patching tools. Shadow IT adds another layer of complexity. One study found the average organization uses 928 cloud-based applications, even though most CIOs think their organization uses only 30 to 40.[4]

Third-party applications. Although many organizations use Microsoft System Center Configuration Manager (SCCM) to update patches, applying it to third-party software that Microsoft does not support requires manual work and testing. Organizations sometimes forego patching virtual servers and other assets due to limited resources.

IN THE FIRST QUARTER OF 2017 ALONE, NEARLY 5,000 SOFTWARE AND SERVER VULNERABILITIES WERE REPORTED.

Time-consuming manual processes. Manual patching processes can consume hundreds of hours every month and are prone to error. If a patch requires a system restart, staff time is stretched even further.

Cultural resistance. Some IT staff may avoid patching certain assets because patches can "break" things, involve extensive customization, aren't always compatible with other applications running on legacy systems, introduce new security problems or add unwanted "bonus" features by default. Despite the critical data held in SAP applications, for example, the average time to patch vulnerabilities after SAP releases a fix is more than six months.[5]

Transforming the Patching Process

Like many organizations in state and local government, the Financial Information System (FIS) department at the University of Pittsburgh must ensure the highest levels of security for financial and personal information in its system. One of its Technical Services team's ongoing tasks is to keep security patches up to date across several hundred applications. Although it manages patch updates through SCCM, popular third-party (non-Microsoft) applications from Adobe, Google, Apple and other vendors required the team to manually detect, build and test patches before deploying them.

"For just three to five applications, we could easily log up to 10 hours per week. Across them all, it was almost a full-time job," says Anthony Digregorio, manager of client computing for FIS Technical Services.

To simplify and expedite third-party patching, the team implemented a solution that automatically detects and updates third-party patches from within SCCM. Instead of visiting each vendor's website to evaluate and download patches, the team can import a single catalog of third-party patches that have been tested and are ready for deployment. Because the patches have already been tested, they are less likely to introduce security problems or unwanted features that may interfere with operations.

With all patch management in a single place, the team can more easily validate compliance. In addition, by slashing the time it takes to update patches from nearly 40 hours to just an hour each week — regardless of how many applications need patching — the team can focus on maintaining its award-winning customer services and delivering new technologies.[6]

BY IMPLEMENTING A SOLUTION THAT AUTOMATICALLY DETECTS AND UPDATES THIRD-PARTY PATCHES, THE FINANCIAL INFORMATION SYSTEM DEPARTMENT AT THE UNIVERSITY OF PITTSBURGH SLASHED THE TIME IT TAKES TO UPDATE PATCHES FROM NEARLY 40 HOURS TO JUST AN HOUR EACH WEEK.

The university's solution is just one example of what automated patching solutions can do. Organizations are also using automated patching to scan for missing patches, discover and patch virtual servers and systems that are not continuously connected to the enterprise network (e.g., laptops), ensure patching is consistently applied across the enterprise, verify patching for auditors, and maintain compliance with the Payment Card Industry Data Security Standard (PCI-DSS) and other regulations that require patch management.

Maximizing the Value of Automated Patching

The following practices help government organizations get the most value from automated patching solutions:

- **Gain C-level sponsorship** to help ensure funding and send the message that patching is an important part of security.
- **Choose an automated solution** that provides a comprehensive, transparent view of the asset inventory and what needs to be patched; scans everything connected to the organization's network; tests and validates patches before they are added to the solution catalog; provides information about the severity of detected vulnerabilities and the criticality of patching; and simplifies reporting to verify patch compliance easily.
- **Commit to a regular patching schedule** that minimizes its impact on productivity and availability (especially for special-purpose machines such as financial servers or web servers). It's also important to establish a clear channel of communication regarding the schedule.
- **Use a multi-tiered process** for deploying patches. Start by updating a subset of machines that are representative of the environment and then correct any problems that arise before deploying patches more widely.
- **Enable transparency and reporting** so IT staff can see which resources are most vulnerable or commonly updated; understand risks; verify patch compliance; and share patch status with colleagues, upper management and regulatory bodies.
- **Develop a defense-in-depth strategy** so other security controls can be used when patches don't exist or will take time to develop.

The Fast Way to Stronger Security

Automated patching not only simplifies and expedites the process, but also ensures patching is applied enterprise-wide. In addition, it allows staff to spend more time on tasks that support the organization's overall mission. As part of a defense-in-depth strategy, patching is a fast way to reduce an organization's attack surface and improve its security posture.

This piece was developed and written by the Center for Digital Government Content Studio, with information and input from Ivanti.

1. http://www.darkreading.com/attacks-breaches/data-breach-vulnerability-data-on-track-to-set-new-records-in-2017/d/d-id/1328947
2. http://info.securityscorecard.com/2016-us-government-cybersecurity-report
3. https://www.symantec.com/content/dam/symantec/docs/reports/gistr22-government-report.pdf
4. Ibid.
5. http://www.pcworld.com/article/2919832/companies-are-falling-behind-on-securing-their-sap-environments.html
6. https://rs.ivanti.com/case-studies/IVI-1236-university-of-pittsburgh.pdf

ivanti

For more information: Phone: 888.253.6201
Email: contact@ivanti.com | Website: www.ivanti.com