Governance of Key Aspects of System Patch Management

When a pop-up notification prompts a user to update their system with the latest patch, the response is often to click on the Remind Me Later option. Then, the normal work routine takes over and later never comes. This approach can put an enterprise at risk if systems are not updated per security recommendations, leading to serious consequences that can disrupt operations.

Patches are intended to repair vulnerabilities or flaws identified after the release of an application or software, upgrade and optimize the system for better efficiency and, most important, mitigate any potential security vulnerabilities. Patch management is often considered a time-consuming and laborious activity and may be neglected even though it is critical for the avoidance of major business disruptions, leading to the compromise of the systems or services. To avoid this, an effective patch management process needs to be established through a comprehensive governance process.

Patch Types

One type of patch is the hot fix, which is designed to address a specific issue identified after the release of software. These patches are not explicitly disclosed and are applied to the system while it is still running, without impacting business operations or requiring a restart of the system. Although hot fixes are limited and rarely occur, they are critical to avoid any business disruptions of the systems or services of the organizations that may be detrimental.

The point release is another type of patch, and it is designed to address a relatively minor error identified in software. No new or additional features are linked with it.

From a business operations perspective, applying the security patch or release of the security patch is the most common process step adopted by organizations, and it is used to make changes in the software to address weaknesses or vulnerabilities identified during regular security scans or tests. The security patch is often considered corrective in nature, as it helps prevent the exploitation of security vulnerabilities. Security patches are often treated as cyclical in nature following the same pattern:

- Identify the vulnerability
- Classify the vulnerability in terms of criticality, which helps prioritize the patch fix
- Apply the remediation
- Mitigate the potential or exploited vulnerability

The service pack is another common type of patch. It constitutes a collection of updates, fixes or feature enhancements in the delivered or implemented software. Installable packages are provided with the release notes and easy to apply by the users.

V. J. SRINIVAS | CISA, CISM, ISO 22301 LA, ISO 27001 LA

Is a subject matter expert on information and cybersecurity, risk management, governance and internal audit processes. Srinivas has worked with cross-industry verticals, sectors and geographic locations for more than 28 years.

"One of the key elements of system maintenance is the establishment of an effective and comprehensive patch management program."

Patch Management

One of the key elements of system maintenance is the establishment of an effective and comprehensive patch management program. This is mandatory for any enterprise that wants to protect itself from known or unknown internal or external threats.

The enterprise's patch management program should include several key areas as part of an effective governance process, including:

- Configuration management
- Patch management consisting of testing and validation
- A backup plan, including an IT disaster recovery plan
- A response plan in case of an incident or failure
- A communication plan
- Compliance and governance

As part of the overall patch management process, each of these key areas must be established in collaboration with cross-functional teams—IT infrastructure, network and operational security, process and asset owners, and delivery teams comprising application and database owners or administrators—and with the support of and guidance from enterprise senior leadership.

Configuration Management

Configuration management ensures that systems and applications are available consistently as desired in relation to their performance, functionality, business needs or requirements, and design. Effective configuration management includes:

- The process or asset owner, in coordination with delivery teams, should maintain a functional secure software code library containing the most recently updated and stable software versions used in the delivered or deployed application or system (including configuration files for switches, routers, file servers, database servers and printers).
- Effective and comprehensive system access management controls should be established and maintained to prevent unauthorized access or changes to operational code.
- An updated system hardware asset inventory of all control systems should be maintained by the IT infrastructure team and available only to authorized individuals.
- An updated network architecture should be established and maintained with detailed schematic mapping to identify and locate the power and network cables.
- Detailed documentation of the system configuration should be maintained; this includes keeping system information from the asset inventory in a controlled environment to prevent access by unauthorized internal or external individuals.
- A validated and confirmed system backup with the latest available production environment, including software library, hardware inventory, current configuration and schematics, should be secured and stored in a separate (physical) location and (logical) environment.
- An effective communication process to disseminate updated policies and procedures periodically should be in place.
- An active change and configuration control board should be established to monitor, authorize and control changes to the control system configuration.

Testing and Validation

The testing and validation process plays a significant role as a precursor to patch releases. It ensures that all checks were performed by the stakeholders and that the patch will help mitigate the potential weakness in the system or application to avoid exploitation that leads to the nonavailability of the systems or application. An effective testing and validation process includes:

- Competent and experienced team members should manage the patch management process because it is critical for identifying potential vulnerabilities and mitigating them in a timely manner with near zero business impact or disruption.
- A proactive and preventive approach that is adopted to identify cybersecurity weaknesses, review vulnerabilities and notify relevant

LOOKING FOR MORE?

- Read *Governance Playbook: Integrating Frameworks to Tackle Cybersecurity. https://www.isaca.org/governance-playbook-integrating-frameworks*
- Learn more about, discuss and collaborate on COBIT® and frameworks in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

stakeholders in a timely manner so they can take appropriate action, such as applying patches.

- An effective mechanism that is established and maintained to evaluate the criticality of vulnerabilities or risk factors to operations and determine an immediate action plan, such as applying patches or enabling a work-around solution, based on business needs or urgency.
- Close coordination and collaboration with the product vendor's team to avoid potential warranty nullification.

System Backup Plan

Ensuring the availability of systems or application backup is a standard procedure and best practice for most organizations. Having a backup and restoration process helps the organizations to return the systems or application to prepatch state if patch deployment is unsuccessful for any reason.

Backup plans are a critical process that, if ignored, can lead to unavailability of systems or information; therefore, they must be managed by competent and experienced individuals, with oversight by senior management at periodic intervals as part of the governance process. The asset owner, in collaboration with the process or business owner, must maintain a current and functional backup of all systems, per a predefined schedule. This backup should be created or updated before any patching activities. In addition, the backup administrator should take a snapshot of the functional or production system to mitigate any potential loss of system or data.

At a minimum, the backup plan should cover the following aspects and describe them in detail:

- Backup frequency (e.g., daily, weekly, fortnightly, monthly)
- Backup verification procedure (retrieving and validating the availability of backup information and testing its accuracy)
- Backup or snapshot retention period
- Physical location of backup storage
- Identification and classification of backup media

Because execution of the disaster recovery plan or system restoration is critical if patching fails, it is imperative that both these plans be built as part of the system patch management process.

It is also strongly recommended that the enterprise test backup restoration periodically to capture the smallest details, including timelines. This allows the enterprise to implement appropriate corrections and updates to the plan or the overall process, making it easier to perform these activities during a real-time situation; and teams should be equipped with backup restoration equipment and media at both the primary and alternative locations.

> "The communication plan plays a significant role in the overall success of the patch management process."

Incident Response Plan

An incident response plan is a critical tool that provides stakeholders with appropriate guidance of what, where, who, when and how an issue should be handled if it arises.

The trigger for implementation of an incident response plan is an unsuccessful or missed patch management activity. Therefore, it is imperative that an actionable incident response plan be established and maintained. The incident response plan should include:

- Defined timelines for identification of new vulnerabilities
- Assessment of the impact to business systems if a system patch fails or patching is delayed for any reason
- Actionable plans to patch the system to mitigate vulnerabilities, risk factors or, alternatively, a work-around solution if patching fails or is unavailable
- A structured approach to capture the details of the incident from an end-to-end perspective—that is, from the start of the problem to issue resolution
- A feedback mechanism so that lessons can be learned from reported incidents
- An automated ticketing system to capture incident details for ease of reference, communication among participants and creation of an audit trail

- A knowledge database containing incidents within the enterprise or incidents occurring in similar work environments around the globe. This facilitates learning from experience and strengthens the overall patch management process.

Communication Plan

The communication plan plays a significant role in the overall success of the patch management process. It provides direction to all stakeholders (what, when, who, why, where and how) and highlights the relevance of the overall process. As part of delegating various roles and responsibilities, a point of contact must be identified to manage the communication plan. This ensures that all stakeholders adhere to a standardized process.

Compliance and Governance

The effectiveness of the patch management process is validated through mandated periodic compliance checks, including self-assessments, peer reviews and audits, and management reporting as part of the overall governance process. This ensures that participants follow the entire process from beginning to end per the defined workflows.

Key performance indicators (KPIs), service level agreements (SLAs) and operational level agreements (OLAs) should be identified, established and maintained. This facilitates the effective enablement and adoption of the patch management process.

As part of management's periodic reviews, inputs related to patch management activities and outcomes should be compiled and captured in governance and management reports or dashboards. This highlights achievements and challenges in the overall process.

Conclusion

Having a robust system patch management process assures the enterprise that its management is making informed decisions and maintaining its systems with the fewest risk factors or vulnerabilities. Applying patches is not an optional activity; it is key to system security and the overall user experience. Applying patches in a timely and effective manner can prevent security breaches, data theft or loss, and help to mitigate legal or regulatory compliance issues. The root cause of most data breaches is poor patch management. Therefore, enterprises are strongly advised to implement, maintain and manage an effective patch management process.