Daniel Akpovi

Professor Malik A. Gladden

CYSE 280 - Windows Systems Management and Security

Due date: 25 July 2024

Analyzing the Impact of Windows Patch Management on Cybersecurity

Introduction

Cybersecurity has become indispensable for organizations in this era of technology across all kinds of sectors. With today's sophisticated and all-pervasive cyber threats, having strict security practices to protect sensitive data and guarantee Information Technology (IT) systems remain unaltered is paramount. Proper patch management is timely addressing fixes for vulnerabilities to limit the exposure. The research presented here investigates Windows patch management and its potential effects on the cybersecurity postures of organizations to analyze the related fields, including barriers, methodologies, tools (such as IVM), and practices.

Keeping devices patched is critical in protecting against cyber risks and vulnerabilities. Software vendors create patches to fix security vulnerabilities, add new features and functionality, and improve general system performance. Tech giant Intel stresses that the later these updates are applied, the more susceptible systems are to be vulnerable - which is even less secure for an organization (Intel). These unpatched vulnerabilities are available in the publicly released Mitre dataset (https://attack.mitre.org/resources/attack-data-and-tools/) and help to understand how significant it is for Windows systems timeliness patch management, what difficulties making exemplary implementation of patches, and its direct impacts on cybersecurity. It also looks at frameworks and best practices for automating—or, better yet, "optimizing"—the workflow around patch management and how automation in this specific area of overall cyber

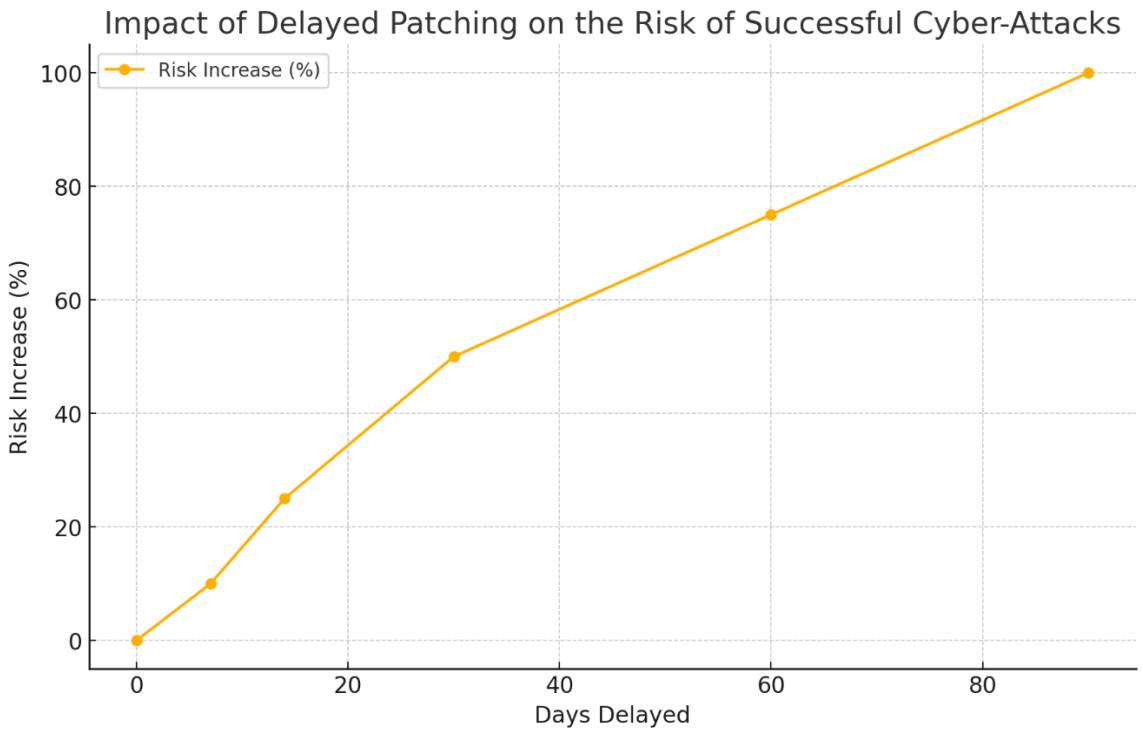
security posture can be viewed as a critical tool to filter out these low-hanging vulnerabilities efficiently.

Overview of the Research /Required Information

Patch management fixes vulnerabilities that threat actors could exploit, and it is an essential component of cyber risk reduction. As a result of increasingly complex IT infrastructures and frequent cyber-attacks, its solutions have evolved from manual operations to automated systems and sophisticated methodologies. According to an article from ManageEngine, a reputable IT management solutions company, within Windows systems, patch management consists of identifying, testing, and deploying updates published by Microsoft to resolve security breaches or improve system performance and functionality ("Automated Patch Management: Process & Benefits"). Emma W, the Head of Advice & Guidance at the UK National Cyber Security Centre, stresses that patch management is essential in cybersecurity as these patches fix targeted vulnerabilities that a lousy actor would otherwise take advantage of to hack, exfiltrate your data, or cause havoc (Emma). For example, the WannaCry ransomware that shook the world in 2017 leveraged an unpatched vulnerability on Windows systems, though a patch had been available months before the attack. Today, Windows patch management includes vulnerability assessments across several vectors and broad-stroke sweeps against various patch testing strategies to deployment designs based on the environment and continual monitoring. Patch management, however, is more complex; organizations find patch management challenging because it is often a choice between security and the need for operational stability while maintaining a very diverse IT environment and minimal disruption to business operations.

Moreover, an article from Acronis observes that the proliferation of IT infrastructures and working from home has made patch management even more difficult (Acronis). Observing a

deep understanding of the vulnerabilities that will be mitigated in patches is necessary. Staying up to date with the latest security advisories, understanding which vulnerabilities can impact an organization's systems, and patch prioritization based on severity and exploitability are all part of securing a system. Black Kite, a reputable cyber risk rating platform, stipulates that organizations commonly automate the identification and prioritization process through vulnerability management tools, allowing them to gain back efficiency in their patch management workflows (Kite). On the other side, patch management or maintenance are not mere technical processes; they need significant organization-wide coordination. Justin Oliver, vice President of Enterprise Technologies at SandStorm IT, advocates that IT and security teams must communicate with business units until everyone understands the importance of patches and the catastrophe that they could lead to. This will encourage the buy-in and resource support system around patch management by creating a culture of security awareness within your organization (Oliver).



The graph above depicts the impact of delayed patching on the risk of successful cyber-attacks. The data shows that the longer patching is delayed, the higher the risk of successful cyber-attacks.

Frameworks / Processes to Follow/Methodology

Patch management is like cleaning; it should follow a well-structured process to ensure all vulnerabilities are found and addressed as quickly and efficiently as possible. Many frameworks and methodologies offer a path to establishing robust patch management processes. An example is the Information Technology Infrastructure Library (ITIL) frameworks and NIST guidelines—which are extensive yet encompass more than just how to handle patches. Organizations should follow a structured lifecycle to manage patches effectively and address several key challenges. Below are the essential steps and considerations for a robust patch management process:

- Steps in the Patch Management Lifecycle
    - Identify: Use scanning tools to identify vulnerabilities in the IT environment and rank their severity.
    - Test: Ensure patches do not introduce new issues or compatibility problems with existing systems.
    - Deploy: Implement patches in a controlled environment.
    - Monitor: Continuously monitor to verify correct installation and detect any subsequent issues (Intel).
- Effective Patch Management Challenges

Organizations have to weigh the necessity of maintaining security against potential risks in deploying patches that could disrupt their operations. In addition, it is very tricky to manage a

diverse IT landscape with different configurations of hardware and software components; changes or modifications must be carefully planned.

- Centralized approach

The article from ManageEngine reports that organizations that adopted a single patch management tool have reported success in quickly responding to the vulnerabilities ("Automated Patch Management: Process & Benefits"). The methodology of effective patch management should also contain regular audits and reviews to check the process. These audits will help identify the gaps and areas that can be improved so that the organization's patch management strategy responds efficiently to newer threats, ensuring that the IT environment changes (Oliver).

- Policy Administration and Enforcement

Beyond the structured procedures, patch management also includes policy administration and enforcing aspects. Organizations need a well-defined policy that covers patch management roles and responsibilities, testing and deployment procedures, and timelines defining when patches should be applied.

Tools/Resources/Results

Many tools and resources are available to help organizations stay on top of patch management, with different tools targeting Small to Medium-sized Businesses/Small to Medium Enterprises (SMBs/SMEs) large enterprises. Some popular patch management tools are ManageEngine, Acronis, and Microsoft System Center Configuration Manager (SCCM). These tools provide features like centralized management, automated patch deployment, and comprehensive reporting capabilities (Acronis). Automation is essential to drive efficiency and effectiveness in patch management. Patch identification, testing, and deployment can be automated by patch management solutions to make applying updates quick and easy. Further,

these tools give actual-time visibility into the patch status of systems together with reporting that assist in ensuring protection policy compliance. Here is a quick comparison of patch management tools plus the popular ones with their strengths and weaknesses. ManageEngine, for example, is a great choice no matter the size of the organization with an easy-to-use interface and strong automation capabilities. On the other hand, Acronis has combined patch management with backup and disaster recovery solutions—supporting a comprehensive cybersecurity strategy. Intel reports that larger enterprises lean toward Microsoft SCCM because of its scalability and integration with other MS products (Intel). The difference between getting a patch management release updated in time or falling behind has tremendous consequences for an organization's security posture. The statistics show that companies with a successful patch management process are less likely to be hacked and have an overall lower risk. According to Kite, the Ponemon Institute reported in a study that organizations waiting at least 30 days to apply patches suffered 60% more breaches than companies that applied these updates (Kite). IT organizations implementing automated patch management tools can also apply patches in less time, require fewer resources, and free up their limited IT staff from a exhausting amount of the manual process. Acronis pointed out that such tools can also enforce the consistent application of patches to all systems, making it less likely that a known vulnerability goes unpatched (Acronis). In ransomware remediation, various other resources can be used for better patch management along with automated tools. For example, services offering threat intelligence can be purchased to provide critical information on new vulnerabilities and exploits as they are uncovered in the wild so that organizations can focus their patching efforts more efficiently. Oliver emphasizes that security training and awareness programs can also help ensure that IT staff are aware of the current best practices in patch management, as well as understand why timely patches need to be

applied (Oliver). It is also possible to perform integrations with third-party security solutions that help improve the capabilities of patch management tools. For instance, patch management and Endpoint Detection and Response (EDR) systems are well suited to make an effective threat management. Frederico Araujo, a researcher at IBM concludes that the integration enables organizations to identify threats that make and model take advantage of unpatched vulnerabilities and react faster (Araujo).

Table comparing the features and capabilities of popular patch management tools.

Feature/Capability	ManageEngine	Acronis	Microsoft SCCM
Automated Patch Deployment	Yes	Yes	Yes
Centralized Management	Yes	Yes	Yes
Comprehensive Reporting	Yes	Yes	Yes
Scalability	High	Medium	Very High
Integration with Other Tools	Yes (Limited)	Yes (Limited)	Yes (Extensive)
Real-time Visibility	Yes	Yes	Yes
User Interface	User-Friendly	User-Friendly	Complex
Supports Multiple OS	Yes	Yes	Yes
Backup and Disaster Recovery	No	Yes	No
Target Users	*SMBs/SMEs	SMBs/SMEs	Enterprises

* Small to Medium-sized Business / Small to Medium Enterprise

The table above compares the features and capabilities of popular patch management tools: ManageEngine, Acronis, and Microsoft SCCM.

Conclusion

Incorporating efficient Windows patch management into an organization's cybersecurity plan is essential. Patches must be applied on time in order to mitigate vulnerabilities and lower the likelihood of successful assaults as cyber threats continue to change and become more sophisticated. The paper presented highlights the importance of following structured frameworks

and methodologies for patch management. It also shows the necessity of a centralized approach, regular audits, and the enforcement of policies. Identifying, testing, and deploying patches can be considerably improved in terms of efficiency and efficacy through the use of automated patch management systems like as ManageEngine, Acronis, and Microsoft SCCM. Organizations can maintain a robust security posture while maintaining operational stability when they use these tools in addition to threat intelligence services and security awareness initiatives. On the other hand, patch management is not without its difficulties, such as the requirement for cooperation throughout the entire business and careful preparation in order to maintain minimal disruptions. It is possible for enterprises to considerably lessen their vulnerability to cyber hazards and potential breaches if they take effective measures to address these difficulties and follow best practices. For the purpose of securing sensitive data and preserving the integrity of information technology systems, it will continue to be vital to be vigilant and to prioritize patch management while the landscape of cybersecurity continues to undergo continuous change.

References

Acronis. “How Does Vulnerability and Patch Management Tie into Cyber Protection?” *Acronis*, 12 Jan. 2021, www.acronis.com/en-us/blog/posts/patch-management-cyber-protection/.

Araujo, Frederico, and Teryl Taylor. “Improving Cybersecurity Hygiene through JIT Patching.” *Proceedings of the 28th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, Nov. 2020, pp. 1421–32, https://doi.org/10.1145/3368089.3417056.

“Automated Patch Management: Process & Benefits.” *www.manageengine.com*, www.manageengine.com/patch-management/automated-patch-deployment.html?mesearch.

Chronopoulos, Michail, et al. “An Options Approach to Cybersecurity Investment.” *IEEE Access*, vol. 6, 2018, pp. 12175–86, https://doi.org/10.1109/access.2017.2773366.

Intel. “What Is Patch Management? Benefits and Best Practices.” *Intel*, www.intel.com/content/www/us/en/business/enterprise-computers/resources/patch-management.html.

Kite, Black. “What Is Patch Management, and How Does It Impact Cyber Risk Management?” *Black Kite*, 5 Oct. 2021, blackkite.com/blog/what-is-patch-management-and-how-does-it-impact-cyber-risk-management/.

Oliver, Justin. “Why Is Patch Management Important for Cyber Security?” *Sandstormit.com*, 23 May 2023, sandstormit.com/what-is-windows-patch-management/.

W, Emma. “The Problems with Patching.” *www.ncsc.gov.uk*, 10 July 2019, www.ncsc.gov.uk/blog-post/the-problems-with-patching.