Journal of
Information Security and Technologies

Research Article Open Access

Vulnerability Management Best Practices: Developing Strategies for Tracking and Remediating Vulnerabilities within Defined SLAs

Santosh Kumar Kande*

Senior Vulnerability Analyst, United states

***Corresponding Author:** Santosh Kumar Kande, Senior Vulnerability Analyst, United States, Tel: +1 203-500-8474, E-mail: kandesantosh9@gmail.com

Received Date: October 05, 2024 **Accepted Date:** November 05, 2024 **Published Date:** November 08, 2024

Citation: Santosh Kumar Kande (2024) Vulnerability Management Best Practices: Developing Strategies for Tracking and Remediating Vulnerabilities within Defined SLAs. J Inf Secur Technol 1: 1-8

Abstract

Vulnerability management has developed into an essential method for minimizing risks and ensure the security of information technology systems in our world which is becoming more and more technologically oriented. With the goal to track and address vulnerabilities within predetermined Service Level Agreements (SLAs), this paper explores the field of Vulnerability Management Best Practices. We establish the importance of vulnerability management in the current cybersecurity environment by looking at the development and history of this field. The importance of asset discovery, risk and patch management, and penetration testing is highlighted as we examine the essential elements of an all-encompassing vulnerability management plan. The article also emphasizes how important it is to prioritize vulnerabilities according to SLA metrics and integrate vulnerability management with other security solutions. It also mentioned about how important it is to track vulnerabilities and fix them within established SLAs, along with automated versus manual remediation techniques. Organizations can improve their vulnerability management procedures and fortify their cybersecurity defenses in the face of emerging threats by aligning SLA metrics with vulnerability severity and promoting continuous monitoring.

Keywords: Vulnerability Management; Service Level Agreements (SLAs); Risk Management; Remediation Strategies; Vulnerability Severity; Vulnerability Prioritization

Introduction

In today's technologically advanced society, there is a growing need for increased vigilance to avoid preventable risks. A key practice in this approach is vulnerable management, which refers to the continuous process of identifying, classifying, prioritizing, and remediating or mitigating security risks within information technology systems [1]. With the growing adoption of different technologies, including the Internet of Things (IoT) [2], note that vulnerability management has become a central component in ensuring that organizations continue to enjoy the benefits of technology, including enhanced efficiency, productivity, and streamlined work processes. The purpose of this research paper is to explore the current best practices in vulnerability management. Specifically, we examine best practices for developing strategies for tracking and remediating vulnerabilities within defined Service Level Agreements (SLAs).

Background and Objectives

Vulnerability management, according to [3], is a layer of information technology security that is aimed at preventing potential risks from becoming a reality. On the other hand, [4] defines vulnerability management as a practice that involves the analysis, identification, and management of potential information technology vulnerabilities. The practice of vulnerability management first originated in the early 1990s, when the number of external threats to deployed IT systems first became a reality for large and established organizations. This is attributed to the fact that before the 2000s, the number of vulnerabilities was significantly small, and therefore, detection and management were generally manual as information security personnel could effectively evaluate and manage threats as they occurred [5]. As such, while the history of vulnerability assessment tools can be traced back as far as the mid-1970s, the practice of vulnerability management became official in the early 2000s when a research program by the MITRE Corporation, funded by the federal government, led to the creation of the Common Vulnerability and Exposure (CVE) system.

The CVE system provided a common reference for publicly known IT vulnerabilities and exposures, which in turn allowed security personnel to adequately respond to such vulnerabilities before their systems could be attacked [6]. However, this approach to vulnerability management changed in the 2010s, when the rate of threats became significantly more common and sophisticated. According to Drake [5], the number of threats grew fourfold by 2005, thereby resulting in the concept of Vulnerability Management (VM). As the threats grew in number, organizations began to rely on vulnerability intelligence in order to prioritize and automate remediation procedures. This approach was characterized by cyclical procedures designed to automate the process of identifying, classifying, prioritizing, and remediating or mitigating potential vulnerabilities in deployed systems [7]. Owing to the growing reliance on software systems to automate different aspects of work and enhance efficiency, vulnerability management has increasingly become an important aspect of modern IT, as it allows organizations to protect themselves against cybercrime and the different related risks [4].

Comprehensive Vulnerability Management

Key components of vulnerability management

A robust and effective threat identification and management plan is essential to ensuring that the organization is able to identify and effectively respond to potential security gaps in their information systems. At the core of effective and robust vulnerability management are the components of a solid information security foundation [8]. Owing to the complexities and challenges of responding to different kinds of cyber threats, many organizations often struggle when it comes to developing the holistic plan needed to address modern, sophisticated, and frequent attacks. According to [9], the secret to a robust and comprehensive VM strategy lies in incorporating specific core elements that are essential to a security strategy.

Key among these components is asset discovery, which is the process of identifying and developing a catalog of all IT assets within the organization's information network [10]. This is considered an important aspect of vulnerability management since the majority of external cyberattacks often occur as a result of vulnerabilities in one or more of the devices attached to the wider network of an or-

ganization [10]. As such, through comprehensive asset discovery, including scanning dynamic endpoints, cloud assets, and bring your own devices, the security team should be able to determine the source of attacks based on the hardware and software connected to their local network based on existing vulnerability information [9].

The second major component of a robust VM strategy is risk and patch management, which refers to the process of deploying relevant security software updates, including firmware, to fix potential vulnerabilities against installed software and hardware [11]. While early detection of potential threats or compromised systems is an essential part of the VM process, it is not until such vulnerabilities are addressed through patch management that the threat can be contained. Finally, an important component of an effective VM strategy is penetration testing, which, according to [12], should be undertaken at least every 12 months to ensure optimal security. Penetration testing involves an authorized simulated cyberattack using the same types of tools, techniques, and processes used by criminals to evaluate and identify potential security risks within an existing IT system [12].

Prioritizing Vulnerabilities

While every security threat in information technology warrants close attention, it is always important to prioritize vulnerabilities based on their potential impact. Prioritization in this respect refers to the process of categorizing and ranking identified vulnerabilities based on likelihood of exploit, business impact, and severity [13]. This process is particularly important in helping security personnel focus their efforts and resources on the most urgent and critical security issues that may have the biggest impact on their organization.

Integrate Vulnerability Management with Other Security Solutions

Effective information security management requires the integration of threat detection and mediation with other aspects of security solutions to ensure a more streamlined approach [14]. A key component in this process is the integration of vulnerability scanning with patch management to allow for easier tracking and management of identified vulnerabilities across the organization's network [15]. For instance, by automating the patching of identified threats, an organization is not only able to promptly respond to threats, but it also improves overall efficiency given the rising number of threats today. Additionally, due to the need to prioritize threats and reduce impact, integration of vulnerability scanning with patch management also allows for better threat response by ensuring that the most important threats are addressed first [14].

Integrating vulnerability management with security awareness training is also an essential step in improving VM strategy [16]. Due to the rise of social engineering as a way of propagating threats, there is a growing need for wider organizational training in order to improve awareness and understanding of the potential sources of security threats [17]. Prevention and reporting procedures should be based on established policies and standards. It is important that the training process be conducted in a manner that communicates the existing information security policies [16]. This highlights the need for integrating vulnerability management with security awareness training, as it not only helps enhance overall awareness of security threats and how to prevent them but also allows employees to better understand the existing information security policies.

Tracking and Remediating Vulnerabilities within Defined SLAs Service-Level Agreements (SLAs)

A key aspect of improving vulnerability management outcomes is tracking and mitigating vulnerabilities with defined service-level agreements (SLAs). As defined by [9], an SLA refers to a contract between an organization and its clients that outlines the types of services to be offered as well as the expected standards of service that the provider is expected to meet. These agreements have become a cornerstone of commercial IT infrastructure given the growing need for reliance on and security of information stored in cloud services [9]. For large and established cloud service providers such as Amazon, Microsoft, and Google, some of the scopes of their SLAs include 100 percent antivirus filtering, 99.9 percent monthly uptime, and 99.9 percent durability of objects over a 12-month period. This means that for a service provider that experiences an uptime of less than 98 percent or security incidents due to

exploits, it is considered a violation since the provider has failed to meet the required standards. In the context of vulnerability management, SLAs provide clear benchmarks for measuring the efficiency and effectiveness of vulnerability response efforts [18].

Remediation Strategies within Defined SLAs

Automated vs. Manual Remediation Approaches

As security threats continue to rise in number and become more sophisticated, organizations involved in the provision of vulnerability management services often face the decision of whether to automate the remediation process for improved efficiency or use manual processes for a more targeted approach [19]. The use of automated remediation approaches has become more common as they allow for rapid identification and patching of identified threats [20]. For instance, intrusion detection and prevention systems (IDS/IPS) are today able to scan and analyze large volumes of data in a significantly shorter time [21]. This enhances the capacity of an organization to identify and promptly respond to potential vulnerabilities, which in turn allows the service provider to meet the standards stipulated in its SLAs.

In addition to speed and prompt identification of potential vulnerabilities, an automated remediation approach is also associated with consistency. This is attributable to the fact that the tools and procedures used in automated remediation often follow predefined rules and processes, which allows for consistency and minimal risks due to human error during the remediation process. Automated remediation is also more scalable when compared to manual approaches that are defined by the availability of skilled security personnel [20]. As such, given the rising number of cyberattacks, automated approaches are more preferable, as they not only provide prompt identification and patching of vulnerabilities but are also more scalable and less prone to human error. This allows organizations to better meet the needs of their clients within stipulated SLAs when compared to manual approaches.

However, although automated tools are powerful aids in vulnerability management, human oversight and decision-making remain essential. This is because certain vulnerabilities, especially new and more sophisticated attacks, are often designed with existing patches in mind [19]. As such, without the intervention of security personnel, such vulnerabilities may not be identified in time. One of the key benefits of the manual remediation process is that it allows security experts to provide contextual insights regarding trends in vulnerabilities and exploits, including the potential impact on specific applications or systems [19]. Additionally, as noted earlier, cyberattacks are becoming increasingly complex and sophisticated, including the use of social engineering to gain access. This highlights the need for human experts who can analyze and provide the insightful information needed to fully understand the potential impact.

Prioritizing Vulnerabilities Based on SLA Metrics

To effectively prioritize vulnerabilities within defined SLAs, organizations must align SLA metrics with the severity and potential impact of each vulnerability. SLA metrics should consider factors such as the exploitability of a vulnerability, the potential damage it can cause, and the assets it could compromise [13]. This allows for a clear ranking of vulnerabilities to be established. Once vulnerabilities are prioritized based on SLA metrics, it is crucial to address high-priority vulnerabilities promptly. High-severity vulnerabilities with a high potential for exploitation pose the most immediate threat to the organization's security. Allocating resources to remediate these vulnerabilities first ensures that critical risks are mitigated effectively and in alignment with SLA objectives.

Continuous Monitoring and Feedback Loop

As noted by [22], vulnerability management is not a one-time effort but an ongoing process that requires continuous monitoring and evaluation. Organizations should regularly assess the effectiveness of their SLAs in tracking and remediating vulnerabilities. If SLA objectives are consistently met, the organization can gain confidence in its vulnerability management program. However, if performance falls short, adjustments to SLA metrics may be necessary to enhance the efficacy of the remediation process.

Based on the insights gained from regular assess-

ments, organizations should engage in an iterative improvement process. This involves continually making data-driven decisions to refine vulnerability management strategies, optimize SLA metrics, and strengthen overall security practices [22]. Through this feedback loop, organizations can evolve and adapt to emerging cyber threats, ensuring that their vulnerability management remains robust and effective.

Asset Discovery Best Practices

Organizations can adopt various tools and methodologies for thorough asset discovery. They should use network scanning tools like Nmap, Qualys, or Nessus to identify devices on their network. Asset management software such as SolarWinds, ManageEngine, or Snipe-IT can help create a comprehensive catalog of assets. Continuous monitoring tools like Security Information and Event Management (SIEM) solutions also aid in asset discovery. Also, Network segmentation must be put into place to reduce vulnerability exposure. It simplifies asset management and security by breaking the network up into smaller sections. And maintaining accurate documentation of all assets, including hardware, software, and their configurations. This documentation helps in tracking changes and ensuring that vulnerabilities are not introduced through unauthorized changes.

Penetration Testing

In order to evaluate an organization's security posture, penetration testing is essential. It assists in locating weaknesses that an attacker might use against you. By taking a proactive stance, companies can address their deficiencies before becoming liable. OWASP Top Ten and SANS Top 25 for web applications for network and infrastructure testing are common techniques used in penetration testing. The outcome will provide a thorough report detailing vulnerabilities found, their severity, and suggested fixes is produced because of penetration testing. It helps companies to identify their exposure to risk, rank their vulnerabilities, and take the necessary steps to secure their systems.

The Human Factor in Vulnerability Management

Human experts are essential for identifying and mitigating complex vulnerabilities, especially those involving zero-day exploits or sophisticated attack techniques that automated tools may not recognize. Security professionals provide contextual insights into the potential impact of vulnerabilities on specific applications or systems. They can evaluate the business impact and advise on the most appropriate remediation actions. Manual intervention is critical for interpreting and responding to emerging threats, such as social engineering attacks. Human experts can recognize patterns and behaviors that automated tools may miss.

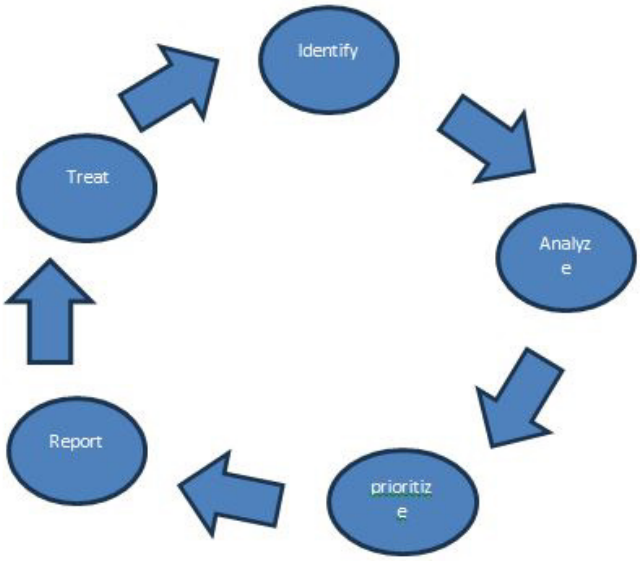

Figure 1: Vulnerability Management Lifecycle

Table 1: SLAs for vulnerabilities based on severity

Severity	SLA
Critical	15
High	45
Medium	60
Low	100

Conclusion

Effective remediation strategies within defined SLAs are essential to ensuring that vulnerabilities are addressed promptly and efficiently. Automated tools can expedite the remediation process, but human oversight and decision-making are vital for more complex vulnerabilities. In essence, by aligning SLA metrics with vulnerability severity and continuously monitoring and adjusting these metrics, organizations can enhance their vulnerability management practices, reducing their risk exposure and strengthening their cybersecurity defenses. The combination of automated and manual approaches, coupled with a commitment to continuous improvement, positions organizations to maintain a proactive stance against evolving cyber threats.

References

1. Arce I (2008) Vulnerability management at the crossroads. Network Security 2008: 11-3.

2. Pompon R, Pompon R (2016) Vulnerability management. IT Security Risk Control Management: An Audit Preparation Plan 165-74.

3. Foreman P (2019) Vulnerability management. CRC Press.

4. Mietala A (2020) When should an organisation start vulnerability management.

5. Drake B (2020) Exploring the Origins and Evolution of Vulnerability Management.

6. Mell P, Grance T (2002) Use of the common vulnerabilities and exposures (cve) vulnerability naming scheme. NIST Special Publication 800: 51.

7. Snell M (2015) History of Vulnerability Management.

8. Awad AI (2018) Introduction to information security foundations and applications.

9. Casola V, De Benedictis A, Rak M (2015, August). Security monitoring in the cloud: an SLA-based approach. In 2015 10th International Conference on Availability, Reliability and Security 749-55.

10. Smyth V (2017) Software vulnerability management: how intelligence helps reduce the risk. Network Security 2017: 10-2.

11. Dissanayake N, Jayatilaka A, Zahedi M, Babar MA (2022) Software security patch management-A systematic literature review of challenges, approaches, tools and practices. Information and Software Technology 144: 106771.

12. Bacudio AG, Yuan X, Chu BTB, Jones M (2011) An overview of penetration testing. International Journal of Network Security & Its Applications 3: 19.

13. Jung B, Li Y, Bechor T (2022) CAVP: A context-aware vulnerability prioritization model. Computers & Security 116: 102639.

14. Adamsky F, Aubigny M, Battisti F, Carli M, Cimorelli F et al. (2018) Integrated protection of industrial control systems from cyber-attacks: the ATENA approach. International Journal of Critical Infrastructure Protection 21: 72-82.

15. Nicastro FM (2011) Security patch management. CRC Press.

16. Yasin A, Liu L, Li T, Fatima R, Jianmin W (2019) Improving software security awareness using a serious game. IET Software 13: 159-69.

17. Ahmad A, Desouza KC, Maynard SB, Naseer H, Baskerville RL (2020) How integration of cyber security management and incident response enables organizational learning. Journal of the Association for Information Science and Technology 71: 939-53.

18. Wu L, Buyya R (2012) Service level agreement (SLA) in utility computing systems. In Performance and dependability in service computing: Concepts, techniques and research directions 1-25.

19. Kupsch JA, Miller BP (2009) Manual vs. automated vulnerability assessment: A case study. In First International Workshop on Managing Insider Security Threats (MIST) 83-97.

20. Jurn J, Kim T, Kim H (2018) An automated vulnerability detection and remediation method for software security. Sustainability 10: 1652.

21. Caliskan M, Ozsiginan M, Kugu E (2013) Benefits of the virtualization technologies with intrusion detection and prevention systems. In 2013 7th International Conference on Application of Information and Communication Technologies 1-5.

22. Anand P, Singh Y, Selwal A, Alazab M, Tanwar S, Kumar N (2020) IoT vulnerability assessment for sustainable computing: threats, current solutions, and open challenges. IEEE Access 8: 168825-53.