|  |  |
| --- | --- |
| MEMO | mercury USA logo |

January 30, 2023

Abdu Kiyaga CMT 421 6380

Dear Judy:

**Overview**

The purpose of this memoranda is to recommend a vulnerability management (VM) process, analyze the OpenVAS vulnerability report, and with an example, highlight business and financial risks if Mercury USA does not carry out or implement the recommendations based on the results of the VM process. The example provided is to cement the importance of a VM process especially in the awake of increased ransomware attacks on logistics companies where attackers take advantage of weaknesses that could be discovered in a vulnerability assessment.

Part 1: Vulnerability Management (VM) Process Recommendation (Nessus)

The most important role of vulnerability management process is to detect and remediate and resolve vulnerabilities in the efficient and timely manner. To be successful at this process, Mercury USA should consider five steps which include: preparation, vulnerability scanning, identifying remediation actions, implementing remediation actions, and rescanning/ ensuring remediation and compliance [1].

The preparation phase, which takes up the first stage, is mostly used to specify the parameters of the vulnerability management program, as well as which systems, IP addresses, and types of scans would be conducted. The resources will be adjusted for a narrower scope based on the IP space and number of hosts discovered by the specified scan. It is advised to start modestly when putting a vulnerability management plan into place. The limited scope will free up the stakeholders to concentrate on carrying out the process rather than being overloaded with vulnerability data from hundreds or thousands of systems [2].

Next, is conducting the initial vulnerability scans where all vulnerabilities should be documented to streamline performance and reliability of scans. This is followed by the remediation phase where data is analyzed determining potential risks and devising means to mitigate such risks before they turn into attack vectors and exploited by attackers. In the final phase of VM assessment, a rescan is performed to ensure that the vulnerabilities on the initial scans have been reconfigured and issues resolved.

To identify vulnerabilities, most industrial players utilize vulnerability scanners such as port scanners and ping scanners. Popular examples include Nessus scanner which would most likely is the scanning program that is advised for use with Mercury USA. With swift, precise scanning and few false-positives, Nessus pinpoints the vulnerabilities that require addressing. In addition, Nessus generates a report highlighting the vulnerabilities, the associated risk and how they could be remediated. Its visually appealing nature of reports using color codes such red for critical vulnerabilities, yellow for medium enables companies to know which vulnerabilities should be prioritized [3].

Typically, industrial recommendations dictate that vulnerability scans should be carried out weekly, and every after three weeks for critical and medium vulnerabilities respectively. The reason behind this is that for critical vulnerabilities, patched may be availed in the weekly Windows patch Tuesday. In addition, Mercury USA in a leader in the logistics industry and it is a target for many attacker, scanning the system weekly ensures that vulnerabilities are caught early and patches applied. The results will be communicated via a vulnerability report presented to stakeholders and Mercury USA business executives.

Part 2: Vulnerability Scanning Tool Evaluation and Recommendations

The VM process tool of use I would recommend is Nessus. This is because the tool can summarize the results of the VM process to a level understood by both technical and non-technical employees by ranking the results based on severity levels. According to the report, the machine on IP address 192.168.1.10 has two results labeled sever; open windows Server Message Block (SMB) sever and hosting software that is no longer supported by Microsoft. Such vulnerabilities can be exploited by attackers to target logistics industries like Mercury USA leading to delayed times to deliver products.

The two recommended scan types are both the authenticated internal and external network scan. An external scan will assist in identifying vulnerabilities that target the local network from the outside. An internal scan provides a snapshot of vulnerabilities that are visible and exploitable from being inside the local network. It is also recommended to perform host based scanning because the scans do not traverse the network and they eliminate network overhead and allow for more continuous scanning. In addition, using external tools such as the Common Vulnerability Scoring System (CVSS) and the Common Vulnerability Exposures (CVE) to collaborate the vulnerabilities with the known attacks and how to prevent them is key to providing remediations [4].

As noted at the beginning of this section, Nessus offers vulnerability screening for mobile devices, web applications and cloud environments in addition to infrastructure vulnerability testing utilizing automatic scan analysis. Additionally, Nessus offers malware detection, embedded device and SCADA auditing, configuration auditing and offering compliance checks.

Part 3: Business Case Example

In this section, provide an example of what could happen if Mercury USA does not implement your recommendations for a VM process (e.g., data exfiltration, hacker intrusions, ransomware, etc.). The text and questions below represent the specifics to focus on while writing your memorandum. Do not include the specific text of the questions in your final submission.

Vulnerability management is an essential part of an organization's success; nevertheless, if Mercury USA decides to go without one, the company will be accepting all possible risks and leaving itself susceptible to several attack vectors. One search attack is the exploitation of the SMB server vulnerability where attackers can remotely log into the system, create new accounts, transfer and encrypt files. This could lead to disruption of work and attackers could ask for ransom for Mercury USA to retrieve its data. This vulnerability was the same that was utilized in the Samba WannaCry attack in 2017 [5].

By implementing a thorough VM program, Mercury USA will be able to quickly address weaknesses in the company system, which might ultimately stop disastrous cyberattacks. Using a systematic, programmatic approach to identifying and addressing risks and vulnerabilities is the greatest way to give yourself a chance of stopping information exploitation and theft.

Closing

To prevent cybersecurity breaches, it is essential to have a vulnerability management architecture in place that often scans for emerging vulnerabilities. Loopholes left on the network for extended periods of time without a vulnerability assessment and patch management mechanism allow adversaries more opportunities to take advantage of flaws and launch attacks as a result. It is therefore important for Mercury USA to adopt the Nessus scanning system to identify, detect and remediate against vulnerabilities on its network. The highlighted risks of not having a solution in place are more of a motivation to have one and keep the network hardened and safe. By doing this, Mercury USA can maintain its growth, productivity, and ability to run a successful firm in the transportation sector.

Best Regards

Abdu Kiyaga  
Cybersecurity Threat Analyst

Mercury USA

References

Use in-text citations in the body of your memorandum as appropriate. Add all sources you used here. This example citation uses IEEE style. Use a style of your choice or ask your instructor for clarification. When using the associated course content, ensure that you cite to the chapter level.

[1] S. Atkinson, "Cybersecurity Tech Basics: Vulnerability Management:1Overview," 2018***.*** [Online]. Available: https://www.cisecurity.org/wp-] content/uploads/2018/07/Cybersecurity-Tech-Basics-Vulnerability-Management-Overview.pdf. [Accessed: 30- January- 2023

[2] "Chapter 5: Implementing an Information Security Vulnerability Management Process", *Pearson CompTIA Cybersecurity Analyst (CySA+)*, 2020. [Online]. Available: https://www.ucertify.com/. [Accessed: 31- January- 2023].

[3] Wendlandt, D. “*Nessus:  A security vulnerability scanning tool”*, n.d [Online]. Available: <https://www.cs.cmu.edu/%7Edwendlan/personal/nessus.html/> [Accessed: 31- January- 2023].

[4] R. Horev, "Winning at Vulnerability Management: 8 Best Practices," 175June 2020. [Online]. Available: <https://securityboulevard.com/2020/06/winning-at-vulnerability-management-8-best-practices/> [Accessed: 29- January- 2023]

[5] Malwarebytes. “*WannaCry: WannaCry was a global ransomware attack in May 2017. Is it still a threat?”,* 2021. [Online]. Available: <https://www.malwarebytes.com/wannacry> [Accessed: 28- January- 2023]