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

January 28, 2023

Reece Zunino CMIT 421 6380

Attn: Judy "Mac" McNamara

**Overview**

Due to a recent cyber-attack on one of our competitors, which resulted in a ransomware attack. The ransomware version that was used in the attack was WannaCry. Due to the nature of the attack on our competitor, our company performed a vulnerability assessment from a third-party pen-tester. We have received the scan report from the company, and this memorandum will address several issues that were found during the scan that requires our immediate attention. Ransomware is software used to hold our data hostage for a sum of money and can make our investors and customers lose trust in our abilities to keep their information safe and secure from outside sources. Our CEO and other personnel's concerns about cyber threats and possible attacks against our company are valid. This memo will discuss recommendations to mitigate the risk we face against a possible attack and provide solutions to some of the issues found in the scan report.

Part 1: Vulnerability Management (VM) Process Recommendation

When creating and Implementing a VM process for mercury USA, we must consider the PCI SSC security standards and regulations regarding the Payment Card Industry to ensure that our customer's data is protected and has met all regulatory guidelines outlined in the PCI-DSS. There have been many updates to the PCI DSS, and the version as of March 31, 2022, is version 4.0. The current version has "requirements for multi-factor authentication (MFA) and is more stringent (Baykara, 2022)".

After ensuring Mercury USA has met all the requirements and standards according to the PCI DSS, we can create internal guidelines and policies tailored to our operations. We would need to begin assessing the existing vulnerabilities of our current technological assets. We would need to conduct our risk assessments based on our company's process, which will determine what is considered critical and not within our infrastructure. When we decide on a crucial asset involved in our operations, we will need to run vulnerability scans routinely at designated intervals according to the guidelines set in the PCI DSS. All scans performed must be credentialed vulnerability scans. These scans may take up more resources but produce better results than non-credentialed scans. These internal scans should be performed monthly due to the constant cyber-attack threats. However, if these scans become too resource-heavy for the company, we must only do quarterly scans to comply with PCI DSS standards strictly.

Cybersecurity professionals use many Scanning tools. Almost all due about the same, but not all are created equally. After researching different vulnerability scanners that are free and open source and others that are paid suites, I would have to recommend Nessus Professional. Nessus was recommended by multiple sites and is in the top 10 recommended by Core Security. "Nessus is trusted by tens of thousands of organizations, with 2 million downloads worldwide (Tenable, 2023)". Nessus may be an annual license that we must buy to update and use the scanning software and it may be expensive. However, I believe the amount of money we would use on a recommended and well-used program will save us more than if we would use a free program that is not as reliable and lose data and our customer's trust.

The scans run by the Nessus program can be tracked and documented easily in reports. These reports can be easily distributed throughout our IT department and be used as a tool on what to focus on in our company's short- and long-term protection. The different IT departments can then also focus on those critical areas of patching security risks that are known CVSS documented vulnerabilities, just like what was found by the OpenVAS scan that the third-party company conducted for us.

Part 2: Vulnerability Scanning Tool Evaluation and Recommendations

The vulnerability scanner used was OpenVAS, also known as green bone. While OpenVAS is a great tool to use, the scan results provided to us by the pen-tester needed to be improved. OpenVAS is a Linux-based scanning tool that is free and is also an open-source, transparent tool. When the tool is used as intended, the scanner can provide very detailed reports and is used and recommended for enterprise systems. However, one of the cons of the vulnerability scanner is that "enterprises will likely need experienced staff to fully extract value from the platform (Keary, 2022)".

With our company needing a tool that is easy to use and can provide more detailed scans, I recommend that Mercury USA acquire the vulnerability scanning tool known as Nessus Pro. Nessus Pro is an easy-to-use scanning tool with the industry's lowest false positive rate with six-sigma accuracy (Keary, 2022). Nessus also has over 50,000 CVEs as well. Many other companies use Nessus because of the low false positive rates and are very successful; in detecting legitimate threats without creating unnecessary work for an administrator to address the issue. The only con for the Nessus Pro vulnerability scanner is that it can be expensive. Still, I believe that the cost is worth it, and this is the tool I would recommend to Mercury USA for our system scanning capabilities.

Part 3: Business Case Example

It is crucial to give context to why our company Mercury USA should implement the recommendations I have laid out above. Here is an example of what could happen if these mitigations and recommendations are not implemented. Currently, the CEO of Mercury USA is aware of the ransomware attack that occurred to our competitor with the WannaCry ransomware. It is unknown to us the extent of the attack on their systems and what data was recovered or, if any, was recoverable. If our company Mercury USA was also hit with such an attack with our current security measures and infrastructure, we would also be facing the same issues of loss of data, customer personal information (PII), bank records of both our customers and us, stored payment information and much more data that could also be proprietary to our company. If all this information gets encrypted by a ransomware attack of any caliber or even just an ordinary hack from a hacktivist or rival company, it would be outing our customers and us at an unnecessary risk that can be mitigated or even prevented with the proper security posture and tools available to monitor and even thwart off such an attack. The fallout from such an attack would lead to a loss of our customer's trust in Mercury USA, possible lawsuits for monetary compensation, or other legal issues that could arise. Failing to protect our customer's best interests and even our own company's best interests could cost us millions of dollars in losses and could be unrecoverable depending on what data was lost.

Now I know that some companies pay the ransom and do get their data back, and sometimes paying off the hackers is cheaper than maintaining a system that is secure from such attacks, but that doesn't always mean that the attackers would give back the data even when they are paid. "Out of all ransomware victims, 32 percent pay the ransom, but they only get 65 percent of their data back (Kochovski, 2022)". This is why it is essential to have tools such as a vulnerability scanner to patch known security threats within a network and monitor those networks for suspicious activity. Nessus Pro is the tool our company needs to keep our customers safe and our company from cyber-attacks.

Closing

It is vital to guarantee a robust and secure infrastructure for Mercury USA against a myriad of cyber threats. It will be in our company's best interest to implement the VM process I have stated above. Keep in mind the example that we went over above and the available statistics of other companies that have gone through a ransomware attack that not all of their data was recoverable, not even with backups, and that overall, recovering from a ransomware attack could cost our businesses $1.85 million on average (Kochovski, 2022) along with losing the customers trust in our company. My recommendation of the vulnerability scanning tool Nessus Pro would be well worth the company's investment over the long run for our security and our customer's knowledge that we take their digital security very seriously and that we take all measures to keep their data safe and secure.

Kind Regards,

Reece Hugo Zunino  
Cybersecurity Threat Analyst

Mercury USA

References

Baykara, S. (2022, September 4). What's new in PCI DSS v4.0? PCI DSS GUIDE. https://www.pcidssguide.com/whats-new-in-pci-dss-v4-0/#:~:text=protecting%20payment%20data.-,PCI%20DSS%20v4.,(MFA)%20are%20more%20stringent

Fortra. (2023). Top 14 Vulnerability Scanners for Cybersecurity Professionals. https://www.coresecurity.com/. https://www.coresecurity.com/blog/top-14-vulnerability-scanners-cybersecurity-professionals

Groot, J. (2021, August 12). What is PCI compliance? Digital Guardian. https://digitalguardian.com/blog/what-pci-compliance

Keary, T. (2022, April 27). Nessus vs OpenVAS. Comparitech. https://www.comparitech.com/net-admin/nessus-vs-openvas/

Kochovski, A. (2022, November 14). Ransomware statistics, trends and facts for 2022 and beyond. Cloudwards. https://www.cloudwards.net/ransomware-statistics/#:~:text=Recovering%20from%20a%20ransomware%20attack,million%20on%20average%20in%202021.&text=Out%20of%20all%20ransomware%20victims,percent%20of%20their%20data%20back

Malwarebytes. (2017). WannaCry. https://www.malwarebytes.com/wannacry

Tenable. (2023). Nessus vulnerability assessment | Nessus®. Tenable®. https://www.tenable.com/products/nessus