ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

Approach to an Efficient Vulnerability Management Program

Sameer Nanda[1], Umashankar Ghugar*[2]

Senior Associate, Cognizant, Kolkata, India[1]

PhD Scholar, Dept. of Computer Science, Berhampur University, India[2]

ABSTRACT: This paper looks at how to tackle with the new trend of complexity in IT infrastructure; security professionals are putting immense effort to transform vulnerability management in capable to tackle risk. The main goal of this study is to modify traditional pattern and adopt the required-modern approach of vulnerability management. This approaches will weight achieve the good result.

KEYWORDS: Vulnerability, Patch availability, Effective remediation and tracking.

I. INTRODUCTION

Now a day's Operational challenges are always associated with a vulnerability management program. However to tackle with the new tendency in Information Technology infrastructure, security professionals are apply effort to convert vulnerability management in capable to tackle risk [1]. Tuning the same into full efficacy can be highly significant and provide great return in investment if implemented carefully and adjusted regularly [2]. The Organization need to modify traditional pattern and adopt the required-modern approach of vulnerability management. Following approaches will lead to acquire the best solution.

In this survey paper, we propose Approach to an efficient Vulnerability Management Program. The rest of the paper is organized as follows: In section II Related work is discussed. Section III Adopting a Vulnerability Management Solution is discussed. Section IV concludes this paper.

Fig-01

II. RELATED WORK

As per the [3], Most of the Organization uses active scanning to discovery vulnerabilities, which require a remote scan of each network-attached device. But this approach to vulnerability evaluation is checked. We should avoid using traditional scanning roads to discover vulnerabilities, which follows a remote scanning technique with network attached device as this approach is linked to various limitations such as:

DOI: 10.15680/IJIRCCE.2017. 0506035

- **Access Limits:** Few assets and services are always kept so critical that you might be hesitant to access them to scan being on a falsified anticipation of affect to its availability. This becomes the anomaly of vulnerability appraisal; the assets that need it the most are the ones we are the most reluctant to assess.
- **Asset distribution:** Proper asset inventory is quite a challenging area I have noticed in multiple Organizations. It is always a big challenge to access due to location, such as cloud assets or mobile assets like laptops and other mobile devices.
- **Huge information :** The scanners cascade data in the form of long 300, 500 and almost 1000 page report containing long diagrams and tables focusing less visibility on network context specific to the Organization.

Analysis & Validation: As per the [4], Critical risks are specific to every Organization Automated analysis of vulnerabilities allows subsequent prioritization to focus on the critical risks and reduces waste of time chasing low-risks findings. The intention is to create a Fast Track list of action items to be executed quickly to eliminate risk of getting exploited by attackers.

Intelligent Risk Rating: Vulnerability that actually poses a significant risk with limited IT resources, one needs to prioritize identified vulnerabilities to target remediation efforts. Traditional approach focuses on pre-defined severity rating and asset importance based on CVSS. But this is not specific to any organization rather is a generic approach. Asserting that the criticality of vulnerability should hover around several factors, including existing security controls, threat data, the business asset, and the impact of a potential attacks [5].

- First, you need to determine whether the vulnerability is threatening an important system or not?
- Second you need to determine the likelihood of the same getting exploited.
- Third you need to determine impact analysis; what will happen if the vulnerability is exploited? Or will it be considerable, taking down a critical system or extending to other assets?
- Fourth analyze the attack simulation technology in a lab environment to identify what would happen if the steps are put together.

  The generic severity might be different to your Organization. E.g. if an asset runs an application that is crucial to maintaining the business and requires continuous availability, a medium-level vulnerability that threatens to disable this asset might be a critical/high-level risk to this particular business.

Effective Remediation and Tracking: The final and the most important step is to remediate the discovered vulnerabilities. For effective vulnerability management program remediation should be integrated into solution and must consider all available security controls [6].

- **Patch Availability:** Can a patch be deployed or is it “Unpatchable” due to system integration issues, location, availability requirements, custom application limitations, etc[7].
- **System's Susceptibility:** Are you able to reconfigure the network or change access controls to mitigate the vulnerability?
- **Availability Of Other Security Controls:** If a patch is not available, are there other security controls that may provide protection such as firewalls, IPS or anti-malware signatures, or other defences?

As per the [7][8], Remediation must consider all security controls, not just patching, and the availability of security controls should be part of the prioritization process. E.g. when you have a list of critical vulnerabilities for your organization, you might prioritize easy-to-remediate vulnerabilities over ones that are resource intensive. This would allow you to get the most protection in the shortest amount of time. The division of labour says security team to find the vulnerability but the network operation and development team to implement the remediation. The vulnerability management program must enable effective communication with relevant IT Operations team, and an integrated workflow should be generated and track remediation process across these teams. To ensure maximum efficacy skilled & trained resources should be incorporated into security team, who can validate and work in parallel with IT Operations team for vulnerability closure.

Adopting the mentioned approach for a vulnerability management program can definitely reduce risk across one's infrastructure. Find or develop a vulnerability management solution which automates and integrates its process to support the capabilities outlined above. The gaps tracked from the first cycle of vulnerability management must be filled properly and must be used as a lesson learnt for further cycle. The right tool, in the right time, with the right resource along with the right approach will surely enhance the efficiency of your existing or new vulnerability management program.

III. ADOPTING A VULNERABILITY MANAGEMENT SOLUTION

As per the [9][10], to deal with current trend of information security and sophisticated cyber threat we need the most efficient and best suited vulnerability management solution for our infrastructure as well as applications. As vulnerability management deal with people, process and technology; we need to choose each of them carefully. Technology is the pillar which is very vast and we cannot opt for multiple investments on the same. We need to be much cautious while choosing the same .One can take into account following parameters while choosing a vulnerability management solution:

1. **Capability in dealing with Asset Inventory:** Does the solution provide an asset inventory database? Is it feasible to extend the database schema to support additional fields, such as asset classification? If not, can the technology integrate with other asset management solution/repositories?

2. **Coverage capability for multiple environments:** Capability on handling multiple Operating system. What's the breadth and platform coverage of the technology? Many technologies can perform operations against the Windows family of products, but you'll need technologies that can operate in a heterogeneous environment and can support a variety of platforms, applications, and infrastructure devices.

3. **Support for cloud and mobile approach:** Does the organization need a vulnerability management tool that scans cloud services, such as software as a service or infrastructure as a service? One need to think of far sighted approach as well.

4. **Scalability:** What is the scale of scope to be covered in vulnerability management and whether the tool is capable enough to handle the count of scope? Clarity on capability of tool to handle multiple infrastructure devices, applications etc.

5. **Ease of Operation:** A tool that is incommodious to navigate or presents confusing dashboard information won't be used, at least not to its fullest potential. A vulnerability management tool that requires regular maintenance also becomes a problem for staff that's often already overburdened.

6. **Dealing with false positives & severity:** Most of the automated tool flag false positives as some vulnerability might not be relevant to organizations or one need to edit the severity of vulnerabilities as well. Does the tool possess capability to deal with false positives and severity customization?

7. **Integration capability:** What is the feasibility of the tool integration into existing patch management, configuration management, intrusion detection, and/or monitoring tools and services?

8. **Capability of tool to run non-intrusively:** While scanning production infrastructure it is a must to have passive or non-intrusive approach of scan. Whether the tool has capability of safe scan?

9. **Workflow & ticketing system:** Does the product have a workflow system that allows assigning and tracking issues? Can it auto-assign tickets based on rule sets defined (i.e., vulnerability, owner, asset classification, etc.)? These are the must have capability for a vulnerability management solution

10. **Vulnerability research & Update capability:** One need to check; how frequently do the vendor release updates? Does the distribution mechanism leverage industry-recognized security communications protocols? Does the vendor have its own vulnerability research team? How has the vendor responded to vulnerabilities in its own products?

11. **Dealing with Zero day vulnerability:** Does the tool possess capability to deal with Zero day vulnerability? Do the products possess Predicative analysis of the threat in your environment without the need to perform new scanning?

12. **Reporting:** Is the reporting detailed and customizable? Can we generate trend report? What are the report types? Is the output format of report reusable on other tools?

13. **Remediation Policy enforcement:** Does the product provide the capability to designate the selected remediation at varying enforcement levels, from mandatory (required) to forbidden (acceptable risk), via a centralized policy-driven interface?

14. **Technical Support:** Look for vendors that offer 24/7 support, preferably by phone, and find out if customers can expect an immediate response.

15. Pricing and licensing: Many tools provides different category of licensing. One needs to map the requirement in a cost effective manner.

Considering above 15 factors will definitely help to choose the best Vulnerability Management solution specific to the Organization.

IV. CONCLUSION

Without this vulnerability management process the organisation is under risk across one's infrastructure. However adopting the mentioned approach for a vulnerability management program can definitely reduce risk across one's infrastructure.

REFERENCES

1) ISO/IEC, "Information technology -- Security techniques – Code of practice for information security management " .
2) Quays,Vulnerability management for dummies. Chichester: John Wiley & Sons, 2008. EBook.
3) Williams, A and Nicollet, M: Improve IT Security With Vulnerability Management,
4) Edwards, Chandra Estelle, M.A" Finding trust in relational vulnerability: Interpersonal and intrapersonal influences on the intimacy process".
5) Wikipedia.Vulnerability Management. Retrieved from http://en.wikipedia.org/wiki/Vulnerability_management .
6) Akhilesh Surjan , Shimpei Kudo, Juha I. Uitto" Risk and Vulnerability" Sustainable Development and Disaster Risk Reduction, Part of the series Disaster Risk Reduction pp 37-55.
7) H.W.Njogu, LJ, JN kiere " comprehensive vulnerability based alert management approach for large networks" Future Generation Computer System, Volume 29, Issue 1, January 2013, Pages 27–45.
8) S.Furnell " Vulnerability management: not a patch on where we should be?"Network Security, Volume 2016, Issue 4, April 2016, Pages 5–9.
9) https://www.giac.org/paper/gsec/32851/implementing-vulnerability-management-process.
10) West-Brown, Moira J. et. al. Handbook for Computer Security Incident Response Teams (CSIRTS). 2nd ed. Apr. 2003. 15 Aug. 2003. CERT/CC.
11) Matthew Finifter, Devdatta Akhawe, and David Wagner "An Empirical Study of Vulnerability Rewards Programs"
12) http://www.cert.org/archive/pdf/csirt-handbook.pdf
13) http://fr.security.westcon.com
14) W.knowles,D.Prince,D.Hutsion" A survey of cyber security management in industrial control systems" IJCI Protection.
15) http://www.cio.com/article/2379124/secur
16) http://insights.wired.com/profiles/blogs
17) http://fr.security.westcon.com/documents
18) C.Alcarez, S.Zeadallt "Critical infrastructure protection: Requirements and challenges for the 21st century"
19) https://www.trustwave.com/Services/Vulnerability-Management.

BIOGRAPHY

Sameer Nanda received his B.Tech degree in IT from SOA University, Bhubaneswar in 2009 .After completion of his degree; he joined TCS as a Software Engineer. He has 08 years of Industries experience and Now He is Senior Associate in CTS, Kolkata. His research interests are Information security and Network security.

Umashankar Ghugar received his B.E degree in IT from Utkal University,Bhubaneswar in 2006 and M.Tech degree in Computer Science from Fakir Mohan University,Balasore in 2012. He has 07 years of Teaching experience and Now He is PhD Scholar in Department of Computer Science, Berhampur University,Orissa. His research interests are in Computer Networks such as Wireless Sensor Network and Network security. He is currently a member of IACSIT, CSTA, IAENG and IRED. He has published 03 International journal papers and 02 are under review process.