Is the Cost of Performing Vulnerability Scanning a Step Too Far for On-Premises SMEs?

Student : Sailaja Mohanty, C00315736@setu.ie
Supervisor: Paul Barry, paul.barry@setu.ie
Master of Science (MSc.) in Cybersecurity, Privacy and Trust

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

1. Introduction

Small and medium-sized enterprises (SMEs) play a critical role in the global economy, but they often face significant cybersecurity challenges due to limited budgets, small IT teams, and lack of technical expertise. As cyber threats such as ransomware, phishing, and malware attacks continue to increase, SMEs have become common targets because of their weaker security practices and limited resources.

Vulnerability scanning has become an essential component of organisational cybersecurity, as it helps identify system weaknesses before they can be exploited. For SMEs with On-Premises infrastructures, regular vulnerability scanning can improve security by detecting misconfigurations, outdated software, and known vulnerabilities. However, implementing these practices requires investment in tools, infrastructure, and skilled personnel, which can be difficult for SMEs operating under financial constraints.

In practice, the cost of vulnerability scanning is a major concern for on-premises SMEs. Organisations must balance the need for regular security assessments with limited budgets and technical capabilities. While many studies focus on the technical effectiveness of vulnerability scanning, there is limited research on its financial impact and whether the investment is justified for SMEs. Therefore, this study aims to evaluate the cost versus benefit of vulnerability scanning and determine whether it is a practical and cost-effective solution for On-Premises SMEs.

2. Literature Review

Small and medium-sized enterprises (SMEs) face significant cybersecurity challenges due to limited budgets, small IT teams, and lack of technical expertise. Despite these limitations, cyber threats are increasing, making vulnerability scanning an important security practice for identifying system weaknesses before exploitation. However, for on-premises SMEs, the cost of tools, infrastructure, and skilled personnel raises concerns about whether vulnerability scanning is financially feasible.

Vulnerability scanning is widely recognised as an effective method for identifying security weaknesses in systems and networks. Holm et al. (2011) highlight that scanning tools differ in accuracy and effectiveness, while Tung et al. (2013) emphasise the importance of cost-effective tool selection. Similarly, Ejaz and Matthew (2024) argue that SMEs must balance cybersecurity needs with financial constraints. Studies also show that open-source tools can reduce costs, but may still require technical expertise for proper use and maintenance.

SMEs also face practical challenges when implementing vulnerability scanning. Iyamuremye and Shima (2018) note that many SMEs lack the expertise required to deploy complex tools, while Taşkın and Sandıkkaya (2023) highlight that no single security solution fits all SMEs. In addition, vulnerability scanning tools vary in detection capability and reporting quality, and no single tool can identify all vulnerabilities effectively. This makes tool selection and configuration an important factor for SMEs with limited resources.

Research further highlights the importance of integrating vulnerability scanning with risk assessment to improve security decision-making. Studies show that vulnerability scanning can support risk reduction and strengthen overall security posture, but its effectiveness depends on proper implementation and continuous monitoring. However, most research focuses on technical performance rather than cost implications. There is limited research on whether the financial investment is justified for On-Premises SMEs. This study addresses this gap by evaluating the cost versus benefit of vulnerability scanning in SME environments.

3. Research Questions

Question 1 : What are the costs associated with implementing and performing the required vulnerability scanning tools in On-Premises SMEs?

Question 2 : What security benefits are achieved through vulnerability scanning tools, and how do these justify the associated costs?

Question 3: What challenges do SMEs face when adopting vulnerability scanning practices using tools that meet their specific requirements and priorities?

4. Methodology

This study adopts a mixed-method research approach, with a primary focus on a survey-based methodology, combining both qualitative and quantitative methods to evaluate the cost and effectiveness of vulnerability scanning for on-premises small and medium-sized enterprises (SMEs).

The qualitative component is based on a systematic literature review of academic papers, industry reports, and cybersecurity standards. This review helps identify key themes such as vulnerability scanning tools, challenges faced by SMEs, and cost-effective security practices. A comparative analysis is conducted between open-source tools (e.g., OpenVAS, Nmap, OWASP ZAP) and licensed tools (e.g., Nessus, Nexpose, Qualys), focusing on cost, usability, and effectiveness.

The quantitative component is centred on a survey targeting SME professionals, including IT staff and security practitioners. The survey is designed to collect data on tool usage, budget constraints, frequency of vulnerability scanning, and perceived cost-benefit. The collected data is analysed to identify trends and patterns, supporting the evaluation of whether vulnerability scanning is financially justified for on-premises SMEs.

5. Future Work

Future work will focus on evaluating the performance and cost of vulnerability scanning tools in On-Premises SMEs, including open-source and licensed solutions. Key aspects such as detection accuracy, scan coverage, false positives, and configuration effort will be analysed. In addition, the study will examine how tool capabilities vary across different environments, including network, host, and web application scanning.

A survey will be conducted with SME IT professionals to collect data on scanning practices, tool usage, frequency of scans, and operational challenges in real environments. The survey will also capture information on budget limitations, staff expertise, and decision-making factors for tool selection.

Further comparison will assess tools based on usability, integration with existing systems, scan time, and maintenance overhead, as these directly affect SME adoption. The study will also evaluate how effectively these tools support vulnerability prioritisation and remediation processes.

The aim is to develop practical, cost-effective recommendations for implementing vulnerability scanning effectively in resource-constrained SME environments, while ensuring continuous monitoring and improved security posture.

6. References

Ejaz, U. and Matthew, B. (2024) Cost-effective cybersecurity solutions for SMEs: Balancing security needs and budget constraints. Available at: https://www.researchgate.net/publication/392282793

Tung, Y.-H., Tseng, S.-S., Shih, J.-F. and Shan, H.-L. (2013) 'A cost-effective approach to evaluating security vulnerability scanners', IEEE. Available at: https://ieeexplore.ieee.org/document/6665238

Please find all the references by scanning the QR code.