IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 7, July 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1207025 |

Windows Endpoint Security using PowerShell and ADMX

Jayram Bagal, Dipanshu Sendre, Dr. Jayashree Shinde, Prachi Telharkar, Prashant Mhanta

Department of Information Technology, G H Raisoni College of Engineering and Management, (Affiliated to SPPU)

Pune, Maharashtra, India

ABSTRACT: In today's digital landscape, small-scale companies encounter significant challenges in safeguarding their sensitive data against threats due to limited financial resources. Traditional data loss prevention solutions often come with hefty price tags, rendering them inaccessible to such organizations. Our project addresses this issue by designing a user-friendly script that can be easily deployed and managed by non- experts, lowering the barrier to entry for enhancing data security. Our project proposes an innovative approach leveraging PowerShell and ADMX to develop a cost- effective data loss prevention script. This script aims to fortify the security of employee systems without necessitating expensive licenses, offering small- scale companies a practical and affordable solution to enhance their data security posture. By implementing a preventative approach to data loss prevention, small- scale companies can mitigate risks more effectively and avoid the potentially catastrophic consequences of data breaches. This shift in mindset from damage control to risk prevention reflects a strategic investment in the long-term resilience and viability of small businesses in today's increasingly digitized economy.

KEYWORDS: Data security,PowerShell, ADMX, Cost- effectiveness

I. INTRODUCTION

Data Loss and prevention script: Endpoint security for Small Scale Companies is a project for Small companies often struggle to keep their data safe because they can't afford fancy security solutions. mall-scale companies face a myriad of challenges in safeguarding their sensitive data against a growing array of threats. With limited financial resources at their disposal, these organizations often find themselves unable to afford the hefty price tags associated with traditional data loss prevention solutions. As a result, they are left vulnerable to cyberattacks, data breaches, and other security incidents that can have devastating consequences for their business operations and reputation.

Drawing upon the identified restrictions and security requirements, our script offers a comprehensive approach to endpoint security, addressing key areas such as peripheral and device controls, application and software management, access and user control, content and network restrictions, and system security and maintenance.

By leveraging the power of PowerShell and ADMX, we have developed a versatile and cost- effective solution that empowers small-scale companies to fortify their security posture without incurring exorbitant costs associated with traditional data loss prevention solutions. The script provides granular control over various aspects of endpoint security, enabling organizations to implement restrictions such as restricting the installation of unsigned drivers, disabling USB mass storage devices, and blocking access to malicious websites. Additionally, it enhances application and software management by enabling Microsoft Edge SmartScreen, disabling browser downloads, and streamlining Windows Defender virus scan UI.
Access and user control are strengthened through measures such as disabling the registry editor, command prompt, and Guest account.

By focusing on endpoint security, our Software aims to fortify the security posture of small-scale companies by providing protection directly at the employee system level. This approach is particularly well-suited for organizations with limited IT resources, as it minimizes the need for complex network infrastructure while still delivering comprehensive data loss prevention capabilities.

II. BACKGROUND

Security has become an increasingly pressing concern in the global Information Technology (IT) landscape, with a predominant focus on perimeter defense to prevent external threats. However, thereis a notable gap in addressing

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1207025 |

security post- infection, where attackers gain remote access through means like Remote Access Trojans (RATs). The difficulty lies in distinguishing actions of legitimate users from those of malicious actors, making post-infection security measures equally vital as perimeter defense. PowerShell, known for its versatility and integration capabilities with various tools, has emerged as a favored tool in cyber-attacks. Its background operation capabilities enable attackers to blend into normal system usage, evading detection by conventional security measures such as antivirus software, as it's an inherent component of the Windows operating system.

In the contemporary digital landscape, data security stands as a paramount concern across organizations, irrespective of size. While large enterprises can afford sophisticated data loss prevention (DLP) solutions, small-scale companies often grapple with limited resources and expertise, rendering traditional DLP solutions inaccessible. These solutions typically entail complex software and hardware setups, requiring specialized IT personnel for management.

Consequently, many small businesses find themselves ill-equipped to thwart sophisticated cyber threats, leaving their sensitive data vulnerable to breaches. The repercussions of such breaches, ranging from financial losses to reputational damage and regulatory penalties, underscore the critical need for cost-effective and user- friendly data security solutions tailored to small-scale companies. In response to these challenges, our project endeavors to develop an innovative approach to DLP, leveraging PowerShell and ADMX. By harnessing the scripting power of PowerShell alongside the administrative capabilities of ADMX, our aim is to empower small- scale companies to bolster their data security posture without the exorbitant costs associated with traditional DLP solutions. Through this initiative, we aspire to democratize access to effective DLP solutions, thereby enabling small businesses to mitigate the risks of data breaches and safeguard their long-term viability in today's digitally driven economy.

III. OBJECTIVE

In the contemporary digital landscape, small-scale companies confront escalating cybersecurity challenges, necessitating tailored solutions to safeguard their sensitive data. Our research endeavors to address these pressing concerns by focusing on the development of accessible and affordable security measures. With a primary aim of enhancing data protection, our objectives revolve around creating user-friendly data loss prevention (DLP) scripts, providing cost-effective endpoint security solutions, ensuring streamlined deployment and management processes, and promoting proactive security practices.

1. Developing a User-Friendly Data Loss Prevention (DLP) Script: Small-scale companies often lack the resources and expertise to deploy complex data loss prevention solutions. Therefore, our research focuses on developing a tailored DLP script that addresses this gap. By emphasizing user- friendliness, we aim to lower the barrier of entry for small businesses to implement effective data protection measures. We recognize the criticality of data security for these companies and the potential consequences of data breaches, including financial loss and damage to reputation. Our approach involves analyzing existing DLP solutions to understand their limitations and the specific needs of small businesses.

2. Providing Affordable Endpoint Security Measures: Endpoint security is essential for protecting sensitive data on employee systems, particularly in the current landscape of remote work and BYOD policies. However, traditional endpoint security solutions can be prohibitively expensive for small-scale companies. Our research focuses on identifying cost-effective measures that offer robust protection without breaking the bank.

3. Ease of Deployment and Management: Deploying and managing security solutions can be challenging for small business owners and IT staff who may lack the time, budget, or technical expertise. Our research addresses these challenges by focusing on solutions that are easy to deploy and manage. We aim to identify common pain points in existing security solutions and propose strategies for simplifying deployment and management processes. This includes automation, intuitive user interfaces, and comprehensive documentation to guide users through setup and maintenance tasks. By prioritizing ease of use and accessibility, we aim to empower small-scale companies to take control of their cybersecurity without requiring extensive resources or expertise.

4. Promoting Proactive Security Practices: Reactive approaches to cybersecurity are no longer sufficient in today's threat landscape, where data breaches and cyberattacks are increasingly common. Our research emphasizes the importance of proactive security practices in mitigating the risk of data breaches and loss. We advocate for a holistic approach that includes encryption, access control, regular data backups, employee training, and security awareness programs. Our research highlights the role of the DLP script and endpoint security measures in supporting proactive security measures, such as monitoring and enforcing data usage policies, detecting suspicious

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1207025 |

activities, and preventing unauthorized access or data exfiltration. Ultimately, our goal is to empower small-scale companies to adopt proactive security measures as part of their overall cybersecurity strategy, thereby enhancing their resilience to cyber threats.

IV. POWERSHELL AND ADMX

PowerShell and ADMX play crucial roles in managing and configuring systems efficiently and effectively. PowerShell, developed by Microsoft, serves as a versatile scripting language and command-line shell, empowering administrators to automate tasks, configure systems, and manage services across Windows environments. With its extensive library of cmdlets and support for pipelines, PowerShell enables administrators to streamline repetitive tasks and execute complex operations with ease.

Complementing PowerShell's capabilities, ADMX files are integral to group policy management in Windows environments. These files contain administrative policies that define registry- based settings for Group Policy, facilitating centralized management and configuration within an Active Directory infrastructure. By leveraging ADMX files, administrators can enforce policies, control user access, and customize settings for specific components of the Windows operating system, applications, and user profiles. Together, PowerShell and ADMX provide administrators with powerful tools for maintaining system integrity, enhancing security, and optimizing performance in enterprise environments. Whether it's automating routine tasks with PowerShell scripts or fine-tuning system configurations with ADMX-based policies, these technologies play indispensable roles in modern Windows administration, empowering administrators to efficiently manage and maintain their IT infrastructure.

V. LITERATURE REVIEW

A comprehensive exploration of critical facets within the realm of cybersecurity, with a particular focus on data loss prevention (DLP) solutions, endpoint security dynamics, and the automation of security configurations. Through comparative analyses, studies delve into the intricacies of various DLP solutions, shedding light on their effectiveness and cost implications, especially in the context of small businesses where resource constraints are prevalent. Additionally, investigations into the effects of interruptions on user decision quality in endpoint security deepen our understanding of the nuanced interplay between security tools and human behavior, highlighting the need for user-centric approaches in security strategy formulation. Furthermore, the review of emerging trends in DLP technology unveils the latest innovations and best practices, providing valuable insights for organizations seeking to stay ahead of evolving cyber threats. Moreover, practical guides serve as invaluable resources, offering actionable recommendations and strategies tailored to the unique challenges faced by small companies in implementing effective DLP measures. Furthermore, the integration of PowerShell and ADMX amplifies the efficacy and efficiency of system administration practices. PowerShell scripts can be utilized to automate the deployment and management of ADMX-based group policies, facilitating seamless enforcement of security configurations and data loss prevention measures across the organization. This synergy between PowerShell and ADMX empowers administrators to orchestrate complex security workflows, respond rapidly to emerging threats, and optimize resource utilization in pursuit of robust cybersecurity defenses.

As organizations navigate the complexities of safeguarding their digital assets against evolving cyber threats, the combined capabilities of PowerShell and ADMX emerge as indispensable assets in the arsenal of system administrators. By harnessing the power of automation, standardization, and centralized policy management afforded by these technologies, organizations can bolster their resilience to data breaches, mitigate risks, and uphold the integrity and confidentiality of sensitive information.

VI. METHODOLOGY

This research aims to develop and evaluate an Endpoint Security Software (EPS) specifically designed for small and mid-scale companies utilizing Windows Home Edition. These companies often lack the resources for complex infrastructure like Active Directory but require robust endpoint security for employee PCs. Our proposed solution addresses this gap by leveraging Windows Registry modifications to achieve functionalities similar to GPO.

A. Security Features

The EPS will incorporate security features to ensure its own integrity and prevent unauthorized tampering. This may involve password protection for configuration changes and encryption of sensitive data within the registry.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1207025 |

B. User Interface (UI) Design
The EPS will have a user-friendly interface that allows administrators to easily configure security settings. The UI will clearly explain the functionalities achieved through each registry edit.

C. Functionality Testing
We will develop test scenarios designed to mimic essential Group Policy functionalities commonly used for endpoint security. Testing will involve a combination of automated testing frameworks and manual verification to ensure comprehensive coverage.

D. Security Evaluation
Penetration testing and vulnerability scanning will be conducted on the EPS itself to identify and address any potential security weaknesses.

E. Usability Testing
User surveys and usability testing with representatives from target companies will be used to evaluate the user-friendliness and ease of use of the EPS interface.

F. Performance Testing
The impact of the EPS on system performance will be assessed. This may involve measuring resource usage (CPU, memory) and boot times before and after EPS installation.

G. Data Analysis
Data collected during testing will be analyzed to assess the effectiveness of the EPS. This includes:
Success/failure rates for each functionality test. User feedback from usability testing to identify areas for UI improvement. Performance metrics to evaluate the EPS's impact on system resources.

H. Limitations
The EPS will be initially designed for Windows the strategic adoption and adept utilization of PowerShell and ADMX represent pivotal pillars in the pursuit of organizational resilience and security excellence.

I. Research Objectives
Develop an EPS that utilizes secure registry edits to mimic essential Group Policy Editor features on Windows Home Edition. Evaluate the effectiveness of the EPS in replicating core GPO functionalities for endpoint security. Assess the usability and cost- effectiveness of the EPS for target companies.

J. Research Design
This research employs a design science approach, focusing on the development and evaluation of an artifact – the EPS software.

K. Development Process
Programming Language and Environment - The EPS will be developed using a programming language, such as Electron and PowerShell. A user- friendly development environment like Visual code will be utilized.

Registry Key Targeting - We will identify specific Windows Registry keys that control functionalities relevant to endpoint security. These keys will be targeted for modification by the EPS to achieve desired security configurations.

Examples include:
- Disabled CMD
- Restricted installation of unsigned device drivers
- Restricted mass storage device access
- Prevent Windows from Storing LAN Manager Hash (An insecure hashing method)
- Disable Guest Account
- Do not allow enumeration of SAM accounts and shares
- Disabled regedit.exe

Home Edition. Compatibility with other operating systems may require further development. Testing may be limited by the number and scope of test scenarios.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2024 ||

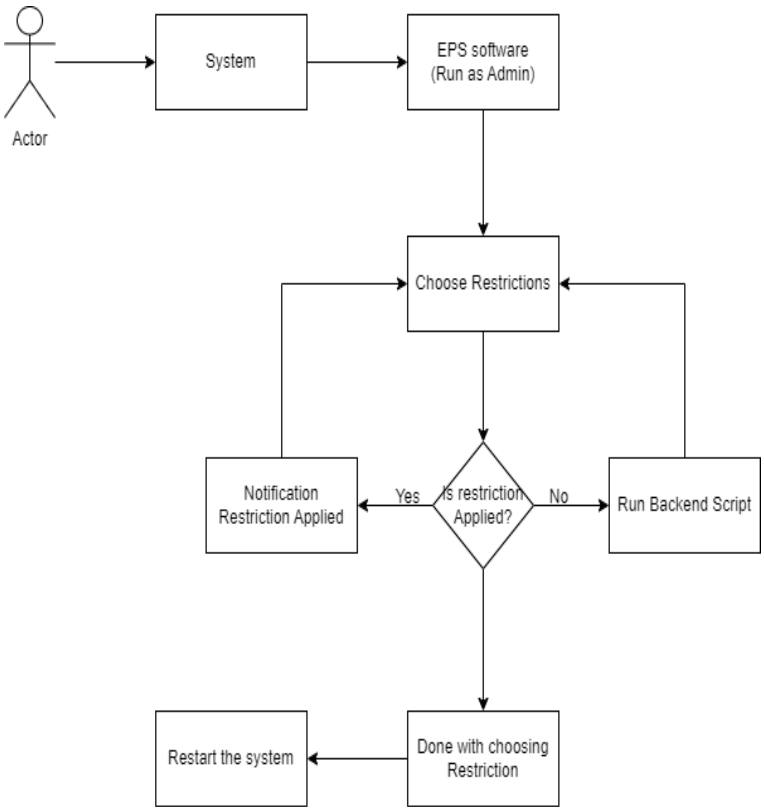
| DOI: 10.15680/IJIRCCE.2024.1207025 |

L. Ethical Considerations

User consent will be obtained before involving participants in usability testing. Data collected during testing will be anonymized and used solely for research purposes.

This methodology outlines a comprehensive approach for developing and evaluating EPS that addresses the security needs of small and mid-scale companies using Windows Home Edition. By focusing on secure registry modifications and user- friendly design, this research aims to provide a cost- effective solution for endpoint security in these organizations.

Architecture



VII. RESULTS

The implementation of these restrictions, in conjunction with the utilization of PowerShell and ADMX, represents a strategic initiative aimed at fortifying data security for small-scale companies operating within constrained budgets. By strategically leveraging these technologies, organizations can effectively address the challenge of securing sensitive data while minimizing financial burdens. By disabling the Command Prompt (CMD), restricting the installation of unsigned device drivers, and limiting access to mass storage devices, organizations can proactively mitigate potential vulnerabilities and thwart unauthorized access attempts. Furthermore, preventing Windows from storing LAN Manager Hash, disabling the Guest Account, and restricting the enumeration of Security Account Manager (SAM) accounts and shares align with the objective of bolstering system defenses against common attack vectors. Additionally, disabling regedit.exe serves as a preventive measure against unauthorized registry modifications, thereby enhancing system integrity and stability. The seamless integration of these restrictions into existing IT infrastructures, coupled with their intuitive user interface and customizable features, underscores their adaptability to the diverse needs of small-scale companies. Overall, the implementation of these restrictions, supported by PowerShell and ADMX, signifies a significant stride towards fortifying data security and instilling trust among stakeholders in an increasingly digitalized environment.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1207025 |

VIII. CONCLUSION

In conclusion, our research underscores the pivotal role of PowerShell and ADMX in providing cost- effective data loss prevention solutions tailored for small-scale companies. By leveraging these technologies, we have not only addressed the challenge of securing sensitive data within constrained budgets but also significantly enhanced system defenses against potential threats. The success of our data loss prevention script highlights its efficacy in mitigating risks while minimizing financial burdens for businesses. Moreover, its seamless integration into existing IT infrastructures, coupled with user- friendly features and customizable options, emphasizes its adaptability to the diverse needs of small-scale companies. This tailored approach empowers organizations to proactively safeguard their data assets, thereby bolstering trust among stakeholders in today's digital landscape. Overall, our findings underscore the importance of strategic technology adoption in fortifying data security, particularly for enterprises with limited resources.

REFERENCES

1. Tianyin Xu, Jiaqi Zhang, Peng Huang, Jing Zheng, Tianwei Sheng, Ding Yuan, Yuanyuan Zhou, and Shankar Pasupathy. 2013. Do Not Blame Users for Misconfigurations. In Proceedings of the Twenty-Fourth ACM Symposium on Operating Systems Principles (Farminton, Pennsylvania) (SOSP '13). ACM, New York, NY, USA.
2. Tianyin Xu and Yuanyuan Zhou. 2015. Systems Approaches to Tackling Configuration Errors: A Survey. ACM Comput. Surv. 47, 4, Article 70 (July 2015), 41 pages.https://doi.org/10.1145/2791577 Preprint Automated Implementation of Windows- related Security-Configuration Guides
3. Microsoft Corporation, "Windows PowerShell (Monad) Has Arrived," [Online].Available: https://devblogs.microsoft.com/powershell/window s- powershell- monad-has-arrived/.
4. Cybersecurity and Infrastructure Security Agency, "Cybersecurity & Infrastructure Security Agency (CISA)FiveHands Ransomware Analysis Report (AR21-126A)," [Online]. Available: https://us-cert.cisa.gov/ncas/analysis-reports/ar21- 126a.
5. Microsoft Corporation "Defending Against PowerShell Attacks," [Online]. Available:https://devblogs.microsoft.com/powershell/defendi ng-against-powershell-attacks.
6. Microsoft Corporation "Security Considerations for PowerShell Remoting using WinRM," [Online]. Available:https://docs.microsoft.com/enus/powershell/scripting/lear n/remoting/winrmsecur ity?view=?powershell-7.2
7. Microsoft Corporation, "Migrating from Windows PowerShell5.1 to PowerShell 7," [Online]. Available:https://docs.microsoft.com/enus/powershell/scripting/wh ats new/migrating-from- windows-powershell-51-to-powershell-

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details