IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, January 2023
Impact Factor: 6.252

Cybersecurity for MSMEs in India: "Analysis of Cyber-Attacks and Implementation of Suitable Security Framework"

Prof. Pravin Patil[1], Ruchika Bhambure[2], Amar Salunke[3], Nitesh Bhujade[4], Shritej Dhadve[5]
Professor, Department of Computer Engineering[1]
Students, Department of Computer Engineering[2,3,4,5]
Zeal College of Engineering and Research, Pune, Maharashtra, India

Abstract: *Micro, small, and medium-sized businesses (MSME) are currently the main targets of cyberattacks in India, yet the fact is that their environment frequently overlooks the prevention of cybercrime. We attempted to introduce a somewhat more robust, self reliant, and efficient cybersecurity solution that can enable higher oppportunity to each individual enterprise's evolving needs and can also quickly adjust with the constantly changing threat environment over the cyber space. Cybersecurity is an environment that is highly demanding and challenging due to the various data transmission layers and the supported IoT devices. The various technologies and tools that can be used to build a cyber security framework specifically for MSMEs are reviewed in this article.*

Keywords: Cyber security, MSME, Cyber Security threats, Cyber Security Framework.

I. INTRODUCTION

Computer science gave rise to the emerging scientific discipline of cybersecurity. The purpose of this study is to extend the existing standard categorical system by proposing a clustering and categorization of current trends in cybersecurity research. The various technologies and techniques that can be used to build a cyber security framework specifically for MSMEs are also described. MSMEs, or micro, small, and medium-sized businesses, are the cornerstone of the Indian economy. It belongs to the ministry of the Indian government- The Ministry of Micro, Small and Medium Enterprises. But they make for the most vulnerable targets in cyberspace.

MSMEs hardly ever perform a cyber-risk assessment, and when they do, they may run into a number of internal problems, such as cyberattacks brought on by inadequate networking security, online fraud, ransomware assaults, etc. A effective first step in cybersecurity risk management has been suggested as mapping MSMEs' present practises and the upcoming risks that need to be tackled with.

II. MOTIVATION

Cybersecurity is the science of mitigating concerns regarding unauthorised access or criminal use of networks that are being used, the peripherals and devices used in the system, and private data. It is also the technique to guarantee the privacy, authenticity, and reliability of information. The fact that there was so little information published about the cyber security of MSMEs, both in India and globally, made our study necessary. There are many frameworks developed for the same, but the National Institute of Standards and Technology Cyber Security Framework is probably one of the most well-known. Our research aims to comprehend the focus of prior MSME cyber security research and identify areas that may be inadequate by using the NIST CSF and CERT India which is administered by Indian Government as a reference. We have carried out a study to analyse the types of cyberattacks and to find out the intensity and risk factor associated with the MSMEs. We carried out a survey for the same and also analysed the survey reports with the existing analysis. We investigated it by using the criteria's given below:

1. Focus of research for MSME cyber security
2. Alignment of previous and current frameworks for MSME-based cyber security
3. Areas that require greater attention
4. The most popular research techniques used for cyber security purpose

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, January 2023
Impact Factor: 6.252

5. Available methods for acquiring data
6. Geographic growth of MSME cyber security research
7. Typical difficulties with implementing MSME cyber security
8. Recommendations and guidelines for MSME cyber security

III. LITERATURE REVIEW

The focus of the research topics and themes were taken into consideration through a qualitative and systematic evaluation of the literature. We opted for the qualitative systematic review approach since completing meta-analyses of studies within a particular topic is challenging. To study and evaluate the integrity of research findings as well as to spot trends and connections across studies on a given subject, qualitative methodologies have been implemented.

The research papers that we selected for our research and literature review purpose were chosen on the basis of criteria as follows-

1. We have taken into consideration only IEEE and equivalent paper sources.
2. All the paper taken into consideration are published 2020 and onwards.
3. The terminologies or keywords mentioned in the considered papers are Cyber security, SME, risk, security awareness, etc.
4. All the considered papers have clearly articulated methodologies.

Except for the research papers and survey papers, we have taken into consideration a few case studies that deals with the cyber security that can be implemented on a small-scale level.

The survey paper that we have chosen to be our base paper for the proposed report is “A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations” authored by Alladean Chidukwani, Sebastian Zander, Polychronis Koutsakis and Published in journal IEEE in the year 2022. The major findings of the survey paper are Contributions by SMBs to the global economy yet the security concerns about the same are very limitedly focused.

Research areas, roles, and classifications for the cyber security framework need more development. Additionally, this publication makes clear reference to future directions, including a focus on SMB cyber security research as well as initiatives and studies to support SMB resilience, which is the direction we have chosen for our proposed study.

The other survey papers and research paper that we have chosen for our proposed system are as follows:

The paper titled “Guidelines and Tool Support for building a cyber security awareness Program for SMEs” authored by Christophe Ponsard and Jeremy Grandchaludon published in the year 2022 in Springer. The major findings of the paper are Guidelines and tools to build a cyber security program and implementing it. and they have mentioned the future scope of their research as initial and final steps of building an awareness program, to create a strategy.

The 2019 IEEE publication by Nikolas Vakalis, Odysseas Nikolis, and Dimosthenis Ioannidis is titled Cybersecurity in SMEs: The Smart- Home/Office Use Case. The main conclusions of the study are "Anomaly identification utilising LSTM model". They also state that the future scope of their research includes evaluation and implementation of "new anomaly detection approaches" along with "Improvement and experimentation with two LSTM models."

Review of cybersecurity research themes, taxonomy, and problems is the title of an article written by Suryotrisongko and Y. Musasash and published in IEEE in 2019. The paper's major findings include categorizing contemporary developments in cyber security technology. Recognition and characterization of home user cybersecurity activity, as well as future interdisciplinary use of their research in numerous industries and technologies.

The study by G. Lloyd, The Business Benefits of Cyber Security for SMEs, was published in Computer Fraud and Security in 2020. The main conclusions of the article are that there are far too many warnings about cyber security dangers and attack outcomes. And they described the intended application of their research as a viable approach that offers small and medium-sized businesses a corporate-level security strategy at a price that is reasonable for every enterprise.

Introducing the human Element into Socio-Technical Cyber Security Risk Assessment is the title of the paper published in the year 2021 by Costas Boletsis and Ragnhild Halvorsrud in the 16th International Joint Conference on Computer Vision. Security threats and the needs to be evaluated in the particular set of circumstances are the article's primary findings. in addition to that, they also proposed the validation case studies with SMEs in several business sectors as the next topic of their research.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, January 2023
Impact Factor: 6.252

IV. SYSTEM ARCHITECTURE

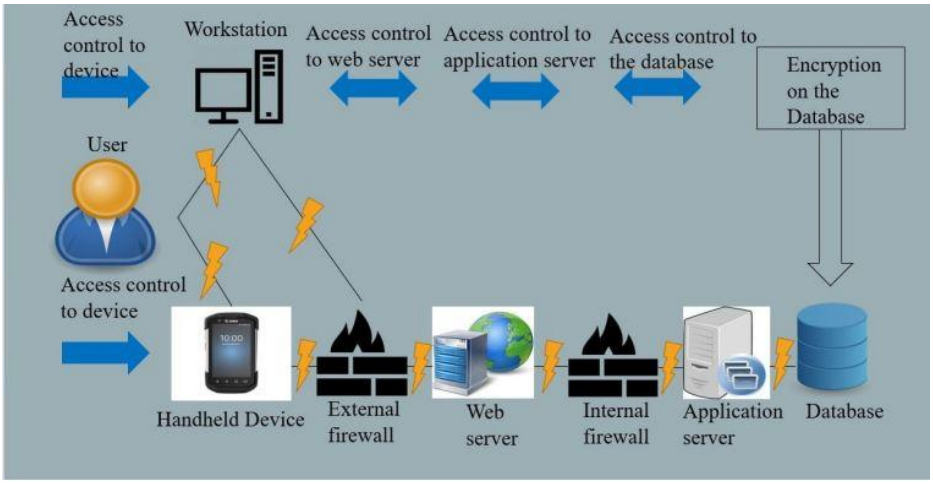

Fig. 1 System architecture of the proposed system

Security mechanisms and countermeasures for your business are integrated into the entire system architecture using a framework called security architecture. The major objective of the controls is to maintain the quality attributes of your key systems, such as privacy, authenticity, and reliability. The interaction of hardware and software is another factor. Understanding, as well as knowledge of programming, research expertise, and ability to create policies In order to protect your company from outside dangers, you must have firewalls, antivirus software, and intrusion detection systems. For your network to maintain and optimise these security technologies, which are already present and functional, your firm should create a comprehensive security architecture including all of these components.

The key features of the above cyber security architecture are the network elements like the protocols used in the network communications and the topologies used in the nodes of the systems as a whole, security elements such as firewalls, etc, cryptographic devices, the security frameworks, standards approved by NIST Risk management framework and security procedures and policies using the industry standard architecture modelling languages.

V. FUTURE SCOPE

Though we have tried to implement a cyber security programmed for the MSMEs in India, there are many aspects that still need to be studied and taken into account in order to understand the threats and implement a better cyber security programme for the MSMEs in India. CJML can be used for cyber security in MSMEs in a number of ways. There are various government schemes that provide financial assistance to MSMEs for cyber security. MSMEs can avail themselves of these schemes to reduce the cost of cyber security. MSMEs can also create awareness about cyber security among their employees. This will help them identify and avoid potential threats. MSMEs can also adopt security policies and procedures to reduce the cost of cybersecurity.

VI. CONCLUSION

In order to promote the development of cyber security solutions, ongoing research is necessary in the industry of MSMEs. Our analysis demonstrates that research in MSME cyber security is fairly constrained and narrowly focused, despite their substantial quantity and significance. This agrees with earlier discoveries made by other researchers. Additionally, we identified that Indian dominated MSME cyber security research is quite low despite other countries having substantial percentage of MSMEs and confronting identical risks but in different circumstances than the Indian MSMEs. Researchers should use more potent, established quantitative research methodologies to examine MSME cyber security in their future work

REFERENCES

[1]. A. Vives, ‘‘Social and environmental responsibility in small and medium enterprises in Latin America,’’ (in English) J. Corporate Citizenship, vol. 2006, no. 21, pp. 39–50, Mar. 2006, Doi: 10.9774/GLEAF.4700.2006.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, January 2023
Impact Factor: 6.252

sp.00006.

[2]. G. Gilfillan. Small Business Sector Contribution to the Australian Economy. Parliament of Australia. Accessed: Apr. 8, 2021. [Online].

[3]. Small Business. What is an SME? Here's an SME Definition. Accessed: Apr. 8, 2021. [Online]. Available: https://www.simplybusiness.co.uk/knowledge/articles/2021/05/what-is-an-sme/

[4]. Organisation-for-Economic-Co-operation-and-Development. OECD Glossary of Statistical Terms-Small and Medium-Sized Enterprises (SMEs). Accessed: Apr. 8, 2021. [Online].

[5]. S. Ward. What Are SMEs? Accessed: Apr. 8, 2021. [Online]. Available: https://www.thebalancesmb.com/sme-small-to-medium-enterprise-definition-2947962

[6]. Australian-Bureau-of-Statistics. Small Business in Australia, 2001. Australian Bureau of Statistics. Accessed: May 13, 2021. [Online]. Available: https://www.abs.gov.au/ausstats/abs.nsf/mf/1321.0

[7]. K. Renaud and G. R. S. Weir, ''Cybersecurity and the unbeatability of uncertainty,'' in Proc. Cybersecurity Cyberfriendships Conf. (CCC), Amman, Jordan, Aug. 2016, pp. 137–143, Doi: 10.1109/CCC.2016.29.

[8]. M. Heikkila, A. Ratty, S. Priska, and J. Jams, ''Security challenges in small- and medium-sized manufacturing enterprises,'' in Proc. Int. Sump. Small-Scale Intel. Manuf. Syst. (SIMS), Larvik, Norway, Jun. 2016, pp. 25–30, Doi: 10.1109/SIMS.2016.7802895.

[9]. C. Onwubiko and A. P. Lenaghan, ''Managing security threats and vulnerabilities for small to medium enterprises,'' Proc. IEEE Intell. Secur. Informat., New Brunswick, NJ, USA, May 2007, pp. 244–249, doi:10.1109/ISI.2007.379479.

[10]. L. Ponemon. What's New in the 2019 Cost of a Data Breach Report. Security Intelligence. Accessed: Jul. 12 2021. [Online]. Available: https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/

[11]. ACSC. Small & Medium Businesses. Australian Cyber Security Centre. Accessed: Aug. 12, 2020. [Online]. Available: https://www.cyber.gov.au/acsc/small-and-medium-businesses

[12]. Better-Business-Bureau. State of Cybersecurity Among Small Businesses in North America. Accessed: May 10, 2021. [Online]. Available: https://www.bbb.org/stateofcybersecurity

[13]. CISA. Security Tip (ST04-001). Cybersecurity & Infrastructure Security Agency. [Online]. Accessed: Mar. 10, 2022. Available: https://www.cisa.gov/uscert/ncas/tips/ST04-001

[14]. H. Suryotrisongko and Y. Musashi, ''Review of cybersecurity research topics, taxonomy and challenges: Interdisciplinary perspective,'' in Proc. IEEE 12th Conf. Service-Oriented Comput. Appl. (SOCA), Kaohsiung, Taiwan, Nov. 2019, pp. 162–167, doi: 10.1109/SOCA.201900031.

[15]. T. Tam, A. Rao, and J. Hall, ''The good, the bad and the missing: A narrative review of cyber-security implications for Australian small businesses,''

[16]. A. Alahmari and B. Duncan, ''Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence,'' in Proc. Int. Conf. Cyber Situational Awareness, Data