International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 12 Issue 8, August 2023, Impact Factor: 7.751

A Study on Introduction to Cyber Security and Its Prevention

Richa[1], Dinesh Dalal[2]

[1]Assistant Professor, Department of Computer Science & Engineering, Faridabad College of Engineering and Management, Haryana, India
[2]Research Scholar, Department of Computer Science & Engineering, Faridabad College of Engineering and Management, Haryana, India

ABSTRACT

This thesis focuses on cyber security by applying data analysis more specifically on real- time data analysis in banking and IT industries in order to identify malware intrusions. Nowadays, information technologies have developed very fast and they have been the main tool that pushes business and economy of every country. Along with all benefits, there are also IT-related risks. Because of the widespread usage of IT in every industry, hackers have become more sophisticated in their methods to attack industries, which rely heavily on information technologies. Many government agencies and industries across the world face cyber threats. Financial services have one of the highest rates of cyber-attacks. In order to fight these cyber threats, banks need to implement different mechanisms, principles, practices, and frameworks in order to improve the internal security. The existing cyber security frameworks provide "what" needs to be done and they do not show "how" it needs to be achieved. Furthermore, many research papers focus on the application of a single analytical method to analyse the data and identify malware. As a result, here is a security standard lack in the IT industry in detecting infections by viruses/malware. This thesis proposes a Malware Detection Framework, which combines different analytical methods and analyses data from various sources in real-time in order to identify malware activities in the Digital world. The developed framework is evaluated through conducting interviews with people who work in the IT industry.

INTRODUCTION

Information technology (IT) has advanced quickly in recent years and is now present in all areas of business. Cyber security risks are a concern for many businesses and governmental organizations around the world (Ikanow Editorial Team, 2014). According to the I Know Editorial Team (2014), this could hurt organizations in a number of ways, including by leading to financial losses, the theft of intellectual property, the unauthorized acquisition of data, and more. According to a 2016 PwC survey, 36% of businesses had dealt with cyber economy crime. The problem of fraudulent behaviour affects every business and every sector of the economy (Campbell & Lautenbach, 2017). Below Figure demonstrates how cybercrime affects every sector of the economy, with the financial services sector having the highest penetration (48%; PwC, 2016).
This article's goal is to develop a framework for security measures in the IT sector. Real-time data analysis is additionally done.

The creation of the Data Security Framework is the focus of the thesis. The focus of the study is the banking business, and more specifically, the penetration of malware, one of the cyber threats facing this sector. The framework that has been created should make it easier to spot this infection and understand where the issue originated.

Because these are preventive measures, staff training and/or malicious software detection are not expressly discussed in the thesis because its objective is to provide a detective/predictive framework for malware identification in organization.

OBJECTIVE OF RESEARCH

The study has been carried out with the following objective:

1. To study and aware the world about the cyber security these days
2. Discuss Some techniques to prevent cyber attacks as early as possible

REVIEW OF LITERATURE

The thesis is concluded in this chapter. The Data Security Framework was created and introduced in this thesis with the goal of identifying malware in the IT industry. The development framework is made up of a number of interconnected layers that communicate by passing information from one to the next. It uses various analytical techniques to spot unwanted intrusions.

The thesis is concluded in this chapter. The Data Security Framework was created and introduced in this thesis with the goal of identifying malware in the IT industry. The development framework is made up of a number of interconnected layers that communicate by passing information from one to the next. It uses various analytical techniques to spot unwanted intrusions. Through examination of the researcher's self-awareness, methodology analysis, and scientific reflection, this part reflects on this paper.

Cyber security is one of the most significant issues now facing businesses, particularly those in the financial sector like banks, which is why I started this study. Since I lack knowledge in this field, it was necessary to analyse numerous research articles and methodologies that other scholars had suggested in order to identify the gap in the literature. The objective of this study was to create a framework that combines several analytical techniques and examines data in real time. This conclusion was reached after going through a number of studies.

The scientific reflection focuses on what this publication has added to the body of "scientific" knowledge, as well as what was discovered about the development process and technique that was used. The Data Security Framework was created in this thesis based on the need and desire for a single multi methodology real-time analysis framework. The many analytical techniques and their combination to improve the identification of harmful activities on the network form the basis of this framework. The L-based Malware Detection Framework places more of an emphasis on "how" than "what," which is where the majority of other frameworks now in use concentrate their attention. The framework suggested various layers that include various elements. These layers can be thought of as steps in a process that are necessary for gathering data, analysing it, and drawing conclusions from the results.

MATERIALS AND METHOD

OWASP Top 10 2021

A non-profit organisation devoted to enhancing software security is known as the Open Web Application Security Project (OWASP). The top 10 most significant web application security threats are ranked in the online publication known as "OWASP Top 10," which also offers repair advice. It reflects a broad agreement onthe most important application security issues. The frequency of security flaws found, the seriousness of the vulnerabilities, and the size of their potential effects are used to rank the risks. The report's goal is to give web application security experts and developers insight into the most common security risks so they can apply the report's conclusions and recommendations to their security procedures and reduce the likelihood that these known dangers will be present in their apps.

SANS TOP 25 Most Dangerous Software Errors

A collaborative research and education institution is the SANS Institute. The mostcommon and significant faults that can result in significant software vulnerabilitiesare listed in the SANS Top 25 Most Dangerous Software Errors (please note: not all vulnerability types apply to all programming languages). The flaws include porous defences, unsafe resource management, and insecure component interaction.
The TOP 25 Most Dangerous Software Errors, according to CWE/SANS, are included in the following table:

Research onion

Research Philosophy: The research philosophy is the topmost layer of the research onion. Important presumptions about the researcher's worldview are contained in this layer . One of the most significant influences is the researcher's personal perception of what constitutes acceptable knowledge . There are four different sorts of philosophical studies:

Studies in positivism observe results and forecast them. In other words, general research philosophies like cause and effect are used in this type of study. They applythe scientific method and put theories to the test with organised, quantifiable facts. Large quantitative sample sizes are used by researchers to produce the desired results

Realists believe that there is a reality that exists separate from the mind. Realisticismand positivism are related in certain ways since they both use the scientific method togenerate knowledge .

Data are gathered for interpretivist studies in the specific areas of a certain subject.They are more prone to study people than things when conducting research .The premise of pragmatic research is that there are various realities and that there is no single point of view that can be used to comprehend the entire picture. The gathering of pertinent information that can support and assist in achieving the intended goal is the fundamental tenet of this research strategy. The year 2013 . Both positivist and interpretivist research methodologies can be combined within a paradigm. The type of the study question will determine how thisis defined .

Research Approach: The two different categories of research methodologies, inductive and deductive, are covered in the second layer of the research onion. The construction of testable theory is a component of the deductive approach . Researchers must create a logical structure based on the definition and assumptions inorder to arrive at the intended result. When the goal is stated, they are predefined . Deductive methods move from the general to the specific .

Research Strategies: Various research methodologies can be used. The inductive approach uses some of these strategies while the deductive approach uses others. Thebest strategy must be chosen in light of the objectives and research questions in order to assist the thesis in addressing them and achieving the goals. It is frequently possible to combine many tactics to speed up the process of getting the desired outcome. Following is a list of every potential tactic along with a brief explanation :

- ***Experiment*:** This type of research focuses on creating a research process that can assess experiment data and compare it to expected results .
- ***Survey*:** Research of this nature is frequently used in quantitative research projects. The output of the survey is data that may be assessed and further quantified .
- ***Case study*:** The study evaluates data that is present in a particular scenario or setting . Additionally, case studies emphasise providing answers to "why," "how," and "what" inquiries .
- ***Action research*:** This is a method for addressing a particular issue within a group of practitioners . It attempts to address a problem that is already troublesome. To advance science, it is essential that the client and the researcher work together .
- ***Grounded theory*:** It attempts to assist studies in behavior prediction and explanation. Consequently, the focus of this technique is on human behavior. Since the data are produced by observations and interviews, the data collecting process begins without the use of any additional framework. Both deductive and inductive methods can use this tactic .
- ***Ethnography*:** Since they are studying people in their natural environment, researchers are obliged to spend a large amount of time immersing themselvesin their lives. In order for the researcher to discover new patterns of what is being observed, the research process must be flexible and time-consuming .*Archival research*: It is done using already-available resources, such as historical documents or literature reviews . To determine the knowledge that already exists in a specific study, the existing data is acquired. The researcher must rely on the data that has been gathered to address a specific issue, but thisdoes not mean that the question will be answered solely using the existing body of literature. Utilizing the available information to create the solution isthe aim of this method .
- ***Design Research*:** All research, whether it is quantitative or qualitative, is predicated on some underlying belief about what makes "legitimate" study andthe best research methodologies, according to Mayer .

Choices: One of the key components that researchers will use is covered by this layer of the research onion. They must choose between using a quantitative, qualitative, ora combination of both method . Researchers have two options: either a single method(mono), which can be either quantitative or qualitative, or a multi-method approach, which combines the two .

Time Horizon: The time horizon that the researchers utilise is covered in the second-to-last layer of the research onion. Studies can be cross-sectional or longitudinal, andboth are possible. A specific subject or issue is addressed by the cross-sectional research. While the longitudinal studies require data to be collected and handled overa longer period of time, they are done for a shorter amount of time. Techniques and procedures: The analysis and acquisition of data, which are based on the methodology approach utilised for the study, form the heart of the research onion

RESULT AND DISCUSSION

The Data Security Framework is built on the use of various data sources and the integration of already implemented analytical techniques. The Framework is all- inclusive and gives a detailed overview of the processes from the data sources throughthe filtration procedure and on to the data characterization

CONCLUSION

The thesis is concluded in this chapter. The Data Security Framework was created and introduced in this thesis with the goal of identifying malware in the IT industry. The development framework is made up of a number of interconnected layers that communicate by passing information from one to the next. It uses various analytical techniques to spot unwanted intrusions. The thesis is concluded in this chapter. The Data Security Framework was created and introduced in this thesis with the goal of identifying malware in the IT industry. The development framework is made up of a number of interconnected layers that communicate by passing information from one to the next. It uses various analytical techniques to spot unwanted intrusions. Through examination of the researcher's self-awareness, methodology analysis, and scientific reflection, this part reflects on this thesis.

Cyber security is one of the most significant issues now facing businesses, particularly those in the financial sector like banks, which is why I started this study. Since I lack knowledge in this field, it was necessary to analyse numerous research articles and methodologies that other scholars had suggested in order to identify the gap in the literature. The objective of this study was to create a framework that combines several analytical techniques and examines data in real time. This conclusion was reached after going through a number of studies. The scientific reflection focuses on what this publication has added to the body of "scientific" knowledge, as well as what was discovered about the development process and technique that was used.

The Data Security Framework was created in this thesis based on the need and desire for a single multi methodology real-time analysis framework. The many analytical techniques and their combination to improve the identification of harmful activities on the network form the basis of this framework. The L-based Malware Detection Framework places more of an emphasis on "how" than "what," which is where the majority of other frameworks now in use concentrate their attention. The framework suggested various layers that include various elements. These layers can be thought of as steps in a process that are necessary for gathering data, analysing it, and drawing conclusions from the results.

REFERENCES

[1]. Aberdeen Group and Wombat Security. (2015). New Research from Aberdeen Group and Wombat Security Confirms Security Awareness and Training Measurably Reduces Cyber Security Risk, (January). Retrieved from https://www.wombatsecurity.com/press-releases/research-confirms- security- awareness-and-training-reduces-cyber-security-risk
[2]. Abuor, J. (2016). Top 5 Security Practices for Financial Institutions to Defeat Online Identity Attacks. Retrieved May 8, 2017, from https://www.linkedin.com/pulse/top- 5-security-practices-financial-institutions- defeat-ken-abuor/
[3]. Advanced Relay Corp. (2017). Banking. Retrieved November 11, 2017, from http://www.advancedrelay.com/w15/markets/banking
[4]. Barracuda Networks Inc. (2017). Barracuda Email Security Gateway. Retrieved from https://assets.barracuda.com/assets/docs/dms/Barracuda_Email_Security_Gateway_ DS_US.pdf
[5]. Constantin, L. (2012). Banking Malware Monitors Victims by HijackingWebcams and Microphones. Retrieved April 25, 2017, from https://www.pcworld.com/article/255979/banking_malware_monitors_victims_by_hijacking_webcams_and_microphones_researchers_say.html
[6]. OWASP TOP 10 Retrieved from https://owasp.org/www-project-top-ten/
[7]. SANS TOP 25 Most Dangerous Software Errors (https://www.sans.org/top25- software-errors/)
[8]. Suryawanshi, A. (2016). Network Traffic Measurements and Analysis using Hadoop, 21–25. Retrieved from http://research.ijcaonline.org/ncacit2016/number3/ncacit3052.pdf
[9]. Zaharia, A. (2016). The Top 10 Most Dangerous Malware That Can Empty Your Bank Account. Retrieved April 21, 2017, from https://heimdalsecurity.com/blog/top- financial-malware/
[10]. Zaian, O. R. (1999). Principles of Knowledge Discovery in Databases. Retrieved June 17, 2017,fromhttps://webdocs.cs.ualberta.ca/~zaiane/courses/cmput690/slides/ch1s.