www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-12, Issue-3, June 2024
Research Paper

Int. J. Sc. Res. in Network Security and Communication

E-ISSN:2321-3256

Protection of Research Data and Devices from Malware Attacks Using Endpoint Security System in Network

Pratap Singh Solanki[1*], Ajay Singh[2], Shaneel Sao[3], N.D. Atkekar[4]

[1,2,3,4]Information Technology Division, CWPRS, CWPRS, Pune, India

[*]*Corresponding Author: solanki_ps@cwprs.gov.in, Tel.: +91-020-24103502*

Received: 15/Apr/2024, Accepted: 18/May/2024, Published: 30/Jun/2024

***Abstract*—**In ealier era, computer were used by limited organizations with limited Internet accessibility therefore data and device security were not big issue. Gradulay, uses of computer increased exponentialy therefore day-by-day it posing new data security challenges. As the uses of Intrenet increases, the challenges of critical data security also increased. Every 39 second, one cyber attack is occurring and thousands website hacked daily. Every establishment uses the computational devices with Internet for running and expnading their business. The computational devices are generting huge volume of data which is very sensitive and essenatial to run the organization. All the devices which are connected in open network are prone to attack by harmful viruses. In this hyper-connected world, protecting the devices and data from loss and unauthorized access are big challenge. The Process of protecting the data from destructive threats, unauthorised access and data corruption is known as data security. In past, the Antivirus software on individual desktop computer were sufficient to protect the device but for various network devices, which are connected in Local Area Network (LAN) is required integrated centralized solution along with management tools. Many antivirus tools sometime failed to detect the advance thretas due to that risk of vulnerability and data lost may increased. End point securiy is an process to protect the all devices which is connected in network. As the Internet uses grown, the types of the threats and techniques changed due to that these Antivirus tools could not prove full efficient to protect the sesitive data. The antivirus software can be used for individual machine but in organization Network, dedicated Endpoint Security System (EPS) is necessary for quickly detecting the malware and common security threats in advance. The EPS runs on organization security policy. The full-proof defence with advanced threat detection system is very necessary. EPS, is an Software System to protect the organization network devices from dectructive threats. It is an device level security system with centralized management and results were encoraging . The End Point Security System provide the security beyond the traditional antiviurs software along with additional features to block the modern threats. In this paper we are discussing about the implementation of Endpoint Security system for protecting computational devices and protecting the scientific and bussiness data at CWPRS Local Area Network (CLAN). The Endpoint Security System has been successfully implemented for protecting the scientific data and devices from external possible thretas.

***Keywords*—** End Point Security System, Virus, Antivirus, Device Protection, Cyber threats, Malware.

I. INTRODUCTION

We are in digital industrialization era where the performance of every Business, Organization and Establishment is digitally evaluated across the world. Information and Commutation Technology (ICT) is the most important strategic issue for any organisation for digital transformation and Network System. Increasingly uses of ICT posing new security challenges. The threats are continuously growing with their complexity. Cyber attacks that can target critical or highly personal information from digital communication network have been a focus of the academic research community for many years [1]. As per CERT-In white papers on India Ransomeware Reprot H1-2022, overall 51% increased in ransomewere incident reported in year 2022-H1 as compare to year 2021. Majority of attacked observed in datacenter, IT, Finance, Manufacturing sector and also targeted the critical infrastrucutres [2]. The unavailability of information may have devastating effect on people, economy, government services and national security. Therefore it is essential to protect the data from external threats. These security for every organization must be consider as essential for functioning of the system and must be dealt with proactive and timely manner. The traditional tools can't protect the data much against the sophisticated and advanced virus attacks.

II. MALWARE

Every day around 56,000 new piece of malwares detected. Malware is a malicious code that installs into the user's computer system without knowledge and performs the malicious activities which may cause lost, steal or corrupt the sensitive data and devices. The computer virus created by the computer programming expert with destructive intention to harm the computer system. The spreading of computer virus is not in the control of human being. The

virus always attached with other program and during execution of program it activates itself and infects the files, eat resource, slow down the system or lock the keyboard. It is type of malware. Computer viruses and worms are characterized by their ability to self replicate. The modern computer virus was conceived and formalized by Fred Cohen as a USC graduate student in 1983. Cohen wrote and demonstrated the first documented virus in November 1983 [3]. Shoch and Hupp invented worms to traverse their internal Ethernet LAN seeking idle processors (after normal working hours) for distributed computing [4]. On November 2, 1988, the famous Morris worm disabled 6,000 computers in a few hours (constituting 10 percent of the Internet at that time) [5]. In March 1999, the Melissa macro virus spread quickly to 100,000 hosts around the world in 3 days, setting a new record and shutting down e-mail for many companies using Microsoft Exchange Server [6]. As per Fred Cohen the computer virus is "a program that can 'infect' other program by modifying them to include a possibly evolved copy of itself". Every program that gets infected may also act as a virus and thus the infection grows [3]. The term Virus and Malware is not identical. The first known self-replicating virus is "Creeper System" which found in year 1971. In year 1986 "Brain" virus was found in DOS operating system. "The Morris" virus spread broadly in year 1988.

Computer virus may spread by opening e-mail attachments, downloading files from un-trusted sites, removable Medium, downloading games, sharing files etc. Due to this the system may have issues like

- Data/File not accessible
- Data lost/steal
- May runs slowly
- Stops responding
- May be crashed or restart automatically
- Applications not accessible or malfunctioning
- Disks or disk drives are inaccessible
- Can't print correctly
- Unusual error messages
- Distorted menus and dialog boxes

As per https://www.getastra.com/blog/security-audit/malware-statistics/, the Malware statistics shows

1. Every day 5,60,000 new pieces of malware are detected.
2. There are now over 1 billion malware programs in existence.
3. Trojans account for 58% of all computer malware.
4. Every minute, four companies fall victim to ransomware attacks.
5. Nearly every second computer in China is infected with some form of malware.
6. Iran has the highest mobile malware infection rate at 30.3%.
7. Android devices are 50 times more likely to be infected with malware than iOS devices.
8. Over the past decade, there has been an 87% increase in malware infections.
9. The cost of cybercrime is predicted to reach $8 trillion in 2023.
10. Open-source vulnerabilities are found in 84% of code bases.

III. ENDPOINT SECURITY SYSTEM

Day-by-day new technology have been developing due to that confidential data are more vulnerable to get the attack. Providing the necessary security to data and device in the Network system in Local Area Network (LAN) is always a major concern to the IT management. The loss of data may affect the business of any organization. As the uses of Internet is growing rapidly, the threats landscape continuously growing quickly. On average every 39 seconds one and daily around 2244 cyber attack happened. The endpoint device is connected with corporate network which is very potential to become the entry point for cyber criminals. This system may be exploited by the attackers to steal or corrupt the confidential data. Endpoint Security is the process of protecting network devices viz. Desktop computer, workstation, Servers and other computational devices from any cyber attacks. As per Gartner, an endpoint protection platform (EPP) is a solution deployed on endpoint devices to prevent file-based malware attacks, detect malicious activity, and provide the investigation and remediation capabilities needed to respond to dynamic security incidents and alerts.

It is essential to deploy solutions that can analyze, detect, and block cyber attacks as they happen. Every endpoint that connects to the corporate network is vulnerability, and becomes the entry point for cyber criminals. Therefore, every device in network carries the risk of becoming the path for hacking into institution. These devices can be exploited by malware that could leak or steal sensitive research data from the business.

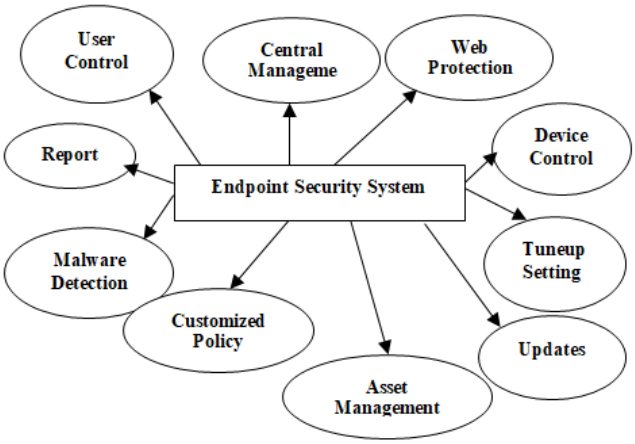

Figure 1.1 : Features of EPS

IV. RELATED WORK

CWPRS is a research organization and became the central agency to cater the R&D needs of the projects in the field of water and energy resources development and water-

borne transport. CWPRS provides specialized services through physical and mathematical model studies in river training and flood control hydraulic structures, harbors, coastal protection, foundation engineering, ship hydrodynamic etc. CWPRS also uses various Network based software Viz. Hydrological and Mathematical Modelling, Remote sensing, Designing software etc. Using CWPRS LAN to execute/study the R&D activities. During these all activities, huge volume of research/study data generated which needs to protect from unauthorized access and data corruption. These generated data are very crucial for National and International level research study and also used to develop the policy towards water resource management. CWPRS receives instruction / guideline from Ministry to implement the Crises Management Plan (CMP) for countering Cyber Attacks & Cyber Terrorism. CWPRS also nominate the nodal officer for Chief Information Security Officer (CISO). Therefore, it is essential to have an advanced centralized data security system to protect the scientific data in CWPRS Network system from external threats. The objective was to have the centralized security system with web-based interface, ease of use and cost-effective endpoint security solution to protect the CWPRS LAN Devices and data from external destructive threats.

These research works are based on the implementation of Endpoint Security System at Central Water and Power Research Station (CWPRS), Khadakwasla, Pune, India. CWPRS is having campus-wide Local Area Network (LAN) which is having more than four hundred computational system and other devices. The LAN and devices are extensively used for accessing e-mail, Internet, e-governance activities, Bio-metric System, Research and Development activities, Mathematical Modeling, Remote Sensing, Government e-Market (GeM), Public Finance Management System (PFMS), e-Payment etc. During execution of various R&D activities, huge volume of critical data is being generated. These scientific data are very sensitive and need to protect. CWPRS was equipped with Antivirus Security System but the product is end-of-life and needs to upgrade for detecting and responding the advanced and modern security threats. The organization applied proactive approach to elevate the data security system to deliver better security outcome and protect the crucial R&D data along with Network Devices and ICT infrastructures.

V. OBJECTIVE

Maintaining critical ICT infrastructure and running the systems all the time with proper security has become a challenging task. All devices are exposed to Internet therefore challenges increased for protecting from the attackers. IT administrator should see for the continuous operations of the networks and computers to the end users for scientific activity. We can follow the standard procedure to maintain the data and IT devices. Every organization should have their own policy as per the needs. As per [7] CERT-in, the main objective of security are, Information is available and usable when required and the system that provide it can appropriately resist attacks and recover from failure (availability). Information is observed by or disclosed to only those who have a right to know (confidentiality). Information is protected against unauthorized modification (Integrality), Business transaction as well as information exchanges between organization locations or with partners/users can be trusted (authenticity and non-repudiation). Keeping in the view the above, the following were the targets to achieve using centralized Endpoint Security System

- Should have Advanced Centralized Endpoint Security system to detect and respond the modern cyber threats.
- Should have centralized web based interface
- Reporting tools
- Remotely installation on client machines
- Should have easy to use and user friendly Single Console Access.
- Asset Management System
- Hardware Change Information to IT Management
- Device Control function
- Network monitoring facility.
- Logs and Report generation.

VI. METHODOLOGY

CWPRS is having campus-wide local area network (TCP/IP based protocol) which spread over an area of 180 hectares and encompasses more than five hundred network devices Viz. Desktop Computer, Servers, Workstation , Network Switches, Network Printer, Bio-metric attendance devices , Wi-Fi routers etc. Optical Fiber Cable (OFC) lay down for providing the network connectivity to the network switches. CWPRS is having 1024 Mbps Internet Lease Line and 34 Mbps NICNET through BSNL. The LAN facility available at various Offices/Divisions share and exchange information over the network through different Servers/Workstation installed in the Data Centre. The Network infrastructure is being extensively used for MIS, Internet/Intranet, Emails, Database Management, AEBAS (Bio-metric), e-Governance activities, PFMS, e-HRMS, GeM, Remote Sensing & Mathematical Modeling, Data Acquisition, Presentation, Library management etc. During the execution of various R&D activities, huge volume of critical data is being generated. These scientific data are very sensitive and need to protect. To protect the IT infrastructures, software, and researched data from unauthorized access and cyber attack, it was essential to upgrade the endpoint security system.

VII. RESULT AND DISCUSSION

CWPRS is now equipped with advanced Endpoint Security system to protect the R&D data and computational devices from the external threats and hackers. The Endpoint Security encompasses all features of antivirus system plus it has new advance feature of full-proof cyber defense with advanced threat detection and response system. The Endpoint Security is giving predictive performance as per organization requirements. The Endpoint Security is facilitated with preventions system, Antivirus /

Antimalware, Central Management, Asset Management, Device Control, Reporting Tools, System Tuneup, Web Protection, Scan Scheduling etc.. The Centralized Management system has user friendly web based management tools/console to see/check the status for client activities. User Logs and various types of Report help a lot to management for supervising and taking the decision. This system also enables to see the complete hardware details/configuration of the nodes connected in network. The system is helping a lot to the network administrator for smooth functioning and protecting the network from external threats. This system also enables us to customize the Policy for protection of critical information and infrastructure using Endpoint Security.

Table 1

Sr. No.	Functions/Features	Benefits to the organization
1.	Central Management	Web based interface to access the centralized console /Dashboard anywhere from the LAN to control the system.
2.	Malware Detection	Advance malware detection system.
3.	Report	Various types of report/ statics help tremendously to take the decision or make the policy.
4.	Customized Policy	We can define the policy as per organization needs.
5.	Asset Management	Provides complete ICT/Hardware device details.
6.	Tune-up Setting	Helps to tune-up the nodes for improving the speed.
7.	Device Control	To control the various plug and play devices.
8.	Web Protection	Web filtering/blocking can be easily handled.
9.	Application Details	Provides the installed application information.
10.	Real-time end point information	Helps to quickly identifying the root cause to troubleshoot.

VIII. CONCLUSION AND FUTURE SCOPE

The discussed in-premises Endpoint Security System is capable to handle the present modern advanced threats/challenges as per R & D Institutional needs. It examine the file, process and report the information about malicious or suspecious acitivity in advance. EPS System also helped to prevent the unintentional and malicious internal action. The EPS also provides the various essenatial ICT hardware and installed application informatoom to the IT Manager. The real-time data collected by EPS of end point devices in network provide the information to quicly idetifying the root cause to troubleshoot. The IT in-charge is now equiped with the tools which helped to continuosly monitoring the entire network system.

ACKNOWLEDGEMENT

Authors are grateful to Dr. R.S. Kankara, Director CWPRS Pune, for institutional support & continuous encouragement and according permission to publish the research paper. The implementation of Endpoint Security System owes its credential due to the constant inspiration rendered by CWPRS users without whom this new technology would have not implemented. I am also thankful to IT Division team for timely suggestions and encouragement in every step.

REFERENCES

[1] Molina-Coronado, B., Mori, U., Mendiburu, A., & Miguel-Alonso, J. “Survey of Network Intrusion Detection Methods from the Perspective of the Knowledge Discovery in Databases Process”, arXiv preprint arXiv:2001.0969, **2020.**

[2] F. Cohen, "Computer viruses: theory and experiments," *Computers and Security*, Feb., Vol.**6**, pp.**22-35, 1987.**

[3] J. Shoch, J. Hupp, "The worm programs - early experience with a distributed computation," Commun. Of ACM, March, Vol.**25**, pp.**172-180, 1982.**

[4] E. Spafford, "The Internet worm program: an analysis," *ACM Comp. Commun. Rev*., Jan., Vol.**19** , pp.**17-57, 1989.**

[5] S. Cass, "Anatomy of malice," *IEEE Spectrum*, Nov., pp.**56- 60, 2001.**

[6] Cert-In, Information Security Policy for protection of critical information and infrastructure CERT-in/NISAP/01, May, Issue.1, **2006.**

AUTHORS PROFILE

Shri Pratap Singh Solanki did his Bachelor of Science (B.Sc.) and Master of Computer Application degree from DAVV University Indore (M.P.). Presently he is working as Scientist-C in Central Water & Power Research Station (Govt. of India, MoJS,DoWR, RD&GR), Khadakwasla R.S. Pune since October 2002. He is having more than 22 years of Industrial, R & D experience in the field of Software Development, Database Management, Water Resource Management & Hydrology, Computer Network, Cyber Security, e-Governance activities, Web Development, Government e-Marketing (GeM) etc.. He has contributed in more than 16 technical research papers in National and International Journals/Conference. He has guided Engineering Graduate students for their project works. He has also delivered more than 20 expert talks in the relevant field at various training program. His area of interest of research is Database Management, Networking, Cyber Security, IoT, Water Resource Management & Hydrology, 5G technologies.

