Methods of managerial, procedural and technical controls for virus and worms

Mihirwalia[1], Siddharth Nanda[2], Rajeshwari Gundla[3]
[1]U.G. Student, SOE, ADYPU, Lohegaon, Pune, Maharashtra, India
[2]Faculty - IT, iNurture, Bengaluru, India
[3]Senior Faculty - IT, iNurture, Bengaluru, India

Abstract- In this networked world, everyone is connected to everyone and same goes for the organizations. Management of these organizations has to measure the upcoming threats due to malwares(Virus and Worms) who can cause loss to the organization. They first analyses the risk without knowing the threat, these risks can be of various types as loss of data, systems, etc. And when the organization is aware of what kind of risk and threat, they are facing they come up with a system to face the issues of the malware. To keep an organization safe from malwares it needs more than technical control, they need to take precautions, manage and train their employees to not to make mistakes because those small mistakes can cause huge trouble for the organization. In this paper we would learn, how can we manage an organization effectively to protect from viruses and worms using managerial, technical and procedural controls.

Keywords- Virus, Worms, risk, malware, threat, controls, managerial, technical, procedural.

I. INTRODUCTION

People sometimes get confused between virus and worm. Virus is a piece of code which attaches itself to a file or program so that it can infect one system to another. Viruses can be of various types as they can damage files, software or hardware. A virus cannot infect a computer unless it's user executes the program it is attached to, similarly it needs human interaction to spread itself. On the other hand, A Worm can spread itself without human interaction and it uses files or information transport features to travel from one computer to another unaided. Worm replicates itself on the primary computer so that it can send many copies of itself to infect many more other computer systems making a huge mess. It is capable to travel through network and can consume system memory causing web servers, network servers and individual computers slow or to stop responding.

II. TYPES OF CONTROLS

a. Managerial / Administrative Control

The personnel responsible for looking out the work and accordingly place controls in check are the information resource manager, network manager or the administrator of the network. The main objective of these personnel is:

b. Configure the Software:

Configure anti-virus for detecting malwares, suspicious code in the system, incoming and outgoing email and data traffic from and to the organization server act accordingly such as raising alert, deletion,etc. Manager should frequently check for updates, upgrades and patches for the software used along with reports for the management.

c. Manage Installations and Documentation:

These personnel are also responsible to manually install and update operating systems and productive tools like MS Office or antivirus tools. Each step has to be documented for the users with reasons as user manual, maintenance process, etc.

d. Regular Checks and Audits:

Regular checks are held so that each and every computer is running the antivirus and has the required software from the authentic sources and not from a non-trusted source. Similarly, reports are generated for every system.

Managers also conduct training programs for the employees with all the user guides and awareness of the modern technical issues(malware) and are strictly maintained to keep the organization safe.

e. Procedural Control

Procedural control is a combination of many procedures set for the users of the system to follow by the managers.These procedures act as precautions to save from malware attacks. These rules are categorized as:

f. Training:

Each organization has a training framework set in place. As the arrival of new installations of softwares or hardwares begin, users need to be aware of its complexions and importance. Hence, each and every user needs to be trained for being aware of risks arising due to the new installations.

g. Admin policies:

The managers need to make certain policies such a not to carry external hard drive or usb drives to the office to access private emails or not to operate private website which can contain malware in it. These policies are to be made clear to the users so that they do not make any mistakes.

h. Data Storage Policies:

Data can be the most important part of an organization, it requires special attention and certain policy of data storage at data center police is essential to ensure smooth functioning of

the system. The procedure for backup and recovery of data is important and should be done from time to time. it depends on the size of data and on the user's level.

i. Physical Security:

Physical security is as important as system security is, system users are also being checked at the entrance and the exit points in case of system usage at high confidentiality establishments like defenseorganization or nuclear plant.

j. Technical Control:

Networks, servers, user access controls, architecture of the system, firewall are the aspects that are being checked, whether they are technically working or not. These controls are defined in policies and procedures of the network and information system teams of the organizations. These are the protection measures undertaken to secure the systems from virus attacks.

k. Network Architecture:

Identify and document all the connections in the network, prepare and update the network diagram to identify other connected networks. make sure all networks isolated if need be and keep the plan ready to isolate any infected network. Keep the known users connected.

l. Firewall:

Create rules and keep the document updated on every rule at the time of installation of a firewall in the system. Rules and procedures are to be implemented with the role assignment of installation. Monitor and generate tracking report at right frequency.

m. Antivirus:

Maintain updated versions of antivirus so that the new malwares in the market can be stopped. Document the software update for the users to use as a manual. Use the recommended procedure of the softwares while installing. Configure it and check the softwares from time to time whether they are working or not.

III. CLASSIFICATION

The goal to eliminate risk factor has been almost successful with our traditional approaches but prevention through technical and procedural control methods can have some sort of risk to it, [1] it is impossible to eliminate the risks completely. Hence organizations should focus more on reducing the impact instead of not having any.

With the use of IPS and IDS, organizations are able to reduce attacks to a minimum. They provide ability to discover intrusion and and arise alert and take strict actions against the attacks. However, [2] recently worms and DDos attacks are getting advanced as well, so they are capable of passing the detection system, hence, to secure the system, organizations need to prevent those attack with firewalls and use technologies like active components in the network infrastructure. Use of ARM(Attack Response Matrix) can help take it a step forward by allowing policies to command actions according to the type and stage of attack. As we know worms spread through network automatically by exploiting the vulnerabilities that can affect a large number of hosts. The speed by which it spread is not healthy for our computer systems, [3] worms can be polymorphic and can change forms while replicating so, it can be difficult to detect the worms in the whole network, for these types of attacks, we might be able to use [2] ARM and can prevent the attack. The other form of worm detection can be by using [4] HoneyStat, It uses honeypots to generates a highly accurate alert stream with low false positive rates. they are script driven, automated and they also cover a large IP space. They generate three class alerts which helps the user to know better about the worms. These are memory alert, disk write alerts and network alerts. If after all these, somehow the malware manages to infiltrate into the network then [5] first thing that should be done is that the compromised computer should disconnect with the network so that it would not spread more than it already has.

IV. FUTURE SCOPE

There are many upcoming organizations in the market and they need to be aware of the danger they can have. This paper is basically to aware them from the problems they can have from viruses and worms, and how to secure themselves from it. They would understand how to manage the company, what procedures to take and which technical aspects to look on. If they utilize these controls effectively, they would be close to being a secure organization because we all know there is no such thing as impenetrable defense.

It can be used in many fields such as Banking, Hospitals, Software developing companies, Universities, E-commerce business, firms, startups, or any organization who uses a servers or is connected to the internet. If the above noted organizations don't adhere to such warnings then there is a huge possibility to be under attack and it can have a huge impact on the organization as the banks or hospitals can lose money or their clients sensitive data which can be used against them respectively. Software development companies can be at loss as their softwarecan be leaked before launch. Hence, every organization need to use these controls to stay secure and protected as much as possible.

V. COMPARISON TABLE

Sr No.	Managerial Control	Procedural Control	Technical Control
1	Manages installations, configurations of softwares, Documentation and audits.	Handles training, admin and data storage policies and physical security of the equipment .	Looks after the network architecture, firewall, antivirus and access controls for users
2	Used for Prevention	Used for Prevention	Used for Detection
3	Manages procedural and technical controls	Precautionary procedures set for the users	Secures the network and protects system from virus

VI. CONCLUSION

We conclude that from this paper that if an organization uses the controls effectively then the loss of data of the organization can get to minimum because the risks from virus and worms cannot be avoided completely.

VII. REFERENCES

[1]. Ashish Garg Ph.D.Jeffrey Curtis, Hilary Halper. (2003) The Financial Impact of IT Security Breaches: What Do Investors Think?.*Information Systems Security* 12:1, pages 22-33.

[2]. Yao-Min Chen, Yanyan Yang, "Policy management for network-based intrusion detection and prevention" , 2004 IEEE/IFIP Network Operations and Management Symposium (IEEE Cat. No.04CH37507).

[3]. Kruegel C., Kirda E., Mutz D., Robertson W., Vigna G. (2006) Polymorphic Worm Detection Using Structural Information of Executables. In: Valdes A., Zamboni D. (eds) Recent Advances in Intrusion Detection. RAID 2005. Lecture Notes in Computer Science, vol 3858. Springer, Berlin, Heidelberg.

[4]. Dagon D. et al. (2004) HoneyStat: Local Worm Detection Using Honeypots. In: Jonsson E., Valdes A., Almgren M. (eds) Recent Advances in Intrusion Detection. RAID 2004. Lecture Notes in Computer Science, vol 3224. Springer, Berlin, Heidelberg.

[5]. Accessed on April 8th,2019 , https://www.cmu.edu/iso/governance/procedures/compromised-computer.html