International Journal of Scientific Research & Engineering Trends
Volume 8, Issue 4, July-Aug-2022, ISSN (Online): 2395-566X

A Study Keen on Computer Network Security Concerns

Mr .Vinayak Pai, Mr. Senthil Jayapal, Anand M, Mr. Jeelani Basha Kattubadi, Dr. Ramesh Palanisamy
Department of CSE,
AJ Institute of Engineering & Technology,
Kottara Chowki, Mangaluru-06, India.
Department of Information Technology,
University of Technology and Applied Sciences,
Ibra, Sultanate of Oman.
Vinayak@ajiet.edu.in, anandm@ict.edu.om, jayapal@ict.edu.om, jeelani@ict.edu.om, palanisamy@ict.edu.om.

Abstract- Network security is a branch of computer security that focuses on computers and networks. Computer security aims to protect information and property against theft, corruption, and natural disasters while keeping it productive and accessible to its intended users. Computer system security refers to the methods and techniques that secure sensitive and essential information and services against dissemination, manipulation, or breakdown due to unauthorized activity, untrustworthy employees, and unanticipated incidents.

Keywords- Computer Security, Network Security, Malware.

I. INTRODUCTION

Viral infections and computer security breaches are all too prevalent these days, so protecting your personal computer has become essential. Consumers' gadgets are more prone to become infected when they connect to the Internet.

Hackers may take sensitive data from a user's device without the user's knowledge. Protecting From these dangers is critical for keeping him healthy and operational for an extended time. Data and software security, which is implemented, using particular applications that link to the computer through the Internet or external storage devices, is the most vulnerable to destruction, hacking, and infiltration (flash memory, disk).

II. LITERATURE SURVEY

Maintaining your computer's security helps you avoid infection and direct and monitor hacking attempts to steal your personal information. Here are a few pointers to help reduce your online risk when you're home on your computer.

Tips for Keeping Your Computer Secure Utilize a firewall. Windows is included, and Antivirus software should be used and updated regularly. If you have a Windows PC, you already have Windows Security or Windows Defender Security Center installed. Make sure your passwords are safe and well-chosen. You were protecting your passwords shows how to do so.

Do not open any suspicious attachments or click on any unusual email links. They can impersonate recognized and reputable sources via emails, tweets, posts, online advertisements, messages, or attachments. People can be found in emails, tweets, postings, online promotions, letters, or extensions, with an automatically activated built-in firewall.

III. DEFINITION OF COMPUTER SECURITY

Information security is an area of technology that applies to computers and networking. Computer security strives to secure information and property against theft, corruption, or natural disasters while being productive and accessible to its intended users. The collective processes and mechanisms by which sensitive and valuable information and services are protected from dissemination, tampering, or collapse caused by unauthorized activities, untrustworthy personnel, and unplanned events are referred to as computer system security terminology.

1. How Is Work Station Security Work?
Safeguard computer and information systems against damage, theft, and illegal usage. It is the technique of identifying and preventing illicit activity computer." A computer crime is an occurrence involving computer security in which a law is broken.

2. PC Security Risks- Unsafe Software:
Those programs let someone get unauthorized access to your computer through the Internet to perform espionage, steal data and information, or damage it.

IV. HACKING

Hacking a computer implies breaking into it regardless of the repercussions. It is cracked, however, when he deletes a file, executes another, or inserts a new one. The hacker can only gain access to your computer if a file called (Patch) or (Patch) is present (Trojan).

V. SPYING LINEUPS

It attempts to identify the contents of the computer, administer it, and carry out various activities, such as installing apps, stealing data and account numbers, passwords, or credit card information, by employing stealth on devices to spy on individuals or entirely control the computer system.

VI. WORM

It is software built by experienced programmers to obtain unauthorized access to a computer with the intent of causing physical component damage and deleting files and programs, leading in a change in the way the computer operates and, in some circumstances, entirely disabling the machine.

VII. SOFTWARE TYPES FOR COMPUTER SECURITY

Antivirus Program offers a different scanning engine that uses heuristic analysis and machine learning to scan, detect, and eradicate even the most sophisticated infestations. Throughout our independent tests, the program regularly surpassed built-in antivirus software in terms of detection and threat avoidance (Windows Defender). One of my favourite aspects of Norton 360, especially the Windows edition, is how easy it is to use and how many complicated options are accessible for more tech-savvy users who want to customize their security. The following features are included with Norton 360: A reliable firewall. Password administrator. Webcam protection.

1. Spyware:
Even though they are not malicious programs, they violate users' privacy by tracking the interests of all Internet users and serving them appropriate adverts.

2. Ransomware:
It is a malicious application that encrypts files or locks the computer, preventing it from functioning entirely or partially, and then displays a screen demanding payment in exchange.

3. Worms:
Worms also self-replicate but do not attach themselves to the host computer's program. The most significant difference between worms and viruses is that worms can quickly move from one computer to another if a network is available, and they do not cause much harm to the target device; for example, worms take up space on the hard disk, slowing down the computer's work.

4. Bots:
They are a more evolved kind of worms, which are automated systems meant to communicate over the Internet without human input, and they can be beneficial or harmful. A malicious bot can infect a single host. Following infection, it will connect to the central server, which will give commands to all infected machines on this connection.

5. Ad-Supported Software:
Although they are not hazardous apps, their proprietors breach users' privacy by tracking all Internet users' interests and serving adverts that are relevant to everyone.

6. Avira:
Avira is one of the most remarkable antivirus engines available, consistently scoring well in independent testing (and scored a 100 per cent spot rate in my tests in general). It is so good that Avira's anti-malware invention has been licensed to several competitors, including Total. Furthermore, because Avira's antivirus engine operates entirely in the cloud, it will not impact the presentation and performance of your gadgets like some other competitors who download large programming packages on your device. Avira Prime has numerous valuable features, such as ongoing malware protection. Ransomware security has advanced. Furthermore, enhanced protection Framework VPN's administrator password, Apps for Android and iOS devices are highlighted.

VIII. SYMPTOMS OF COMPUTER VIRUS INFECTION

- Reload error messages on several systems.
- The notification implies that the cache could not be stored because there is insufficient memory or circular space.
- Other valuable records have been revised and wiped off. An exhausted startup (gadget startup).
- Slow performance with other programs. A few programs will not be utilized. Texts and projects may be transformed into open, limitless possibilities.

1. Virus Prevention:
Activating the firewall system is required for prevention. Install and keep up to date an antivirus application named Antivirus on the computer. It installs a light memory monitoring system on a machine (USB Guard). Before beginning work, test downloaded apps. Use any software or file that you are unfamiliar with. Reduce the number of emails from unknown senders and test them before opening them.Do not download unlawful or trustworthy software, and do not exchange data or programs with strangers or unsuitable people an antivirus application should be used on a regular basis to identify all hard drives. Use no more RAM until Antivirus finds it. Copy data to external drives on a regular basis.

How to get rid of unwanted software including viruses, spyware, and unprogrammed internet security. Computer worm or spyware eradication might be challenging without the assistance of unsuitable computer cleanup software. After viruses and spyware have been found and eradicated, certain computer viruses and other software do not need to be reinstalled. Fortunately, by keeping your computer up to date and employing malware removal solutions, you may assist in the long-term eradication of unwanted software.

2. Prevention:

- Follow these instructions to eliminate a computer virus and other malware.
- Install the most recent Microsoft Updates.
- Note Computer infections might prohibit you from accessing the Microsoft Update Web site and installing the most recent updates. We recommend that you use the Auto Update service so that your machine does not miss any essential updates.
- Make use of Microsoft Antivirus.
- Microsoft offers a free online application that scans and assists in the removal of dangerous dangers from your computer. Go to the Microsoft Antivirus website to run a scan.
- Make use of the Free Windows Computer Software Tool.
- Using the Windows Harmful Software Removal Tool, uninstall a dangerous computer program.
- Remove any previously installed security software.
- If random security software cannot be identified or uninstalled using Microsoft Antivirus or the Windows Software Removal Tool,
- Start Microsoft Defender Offline.

Microsoft Defender Offline is an anti-malware solution that aids in the removal of viruses that begin before Windows viruses. Microsoft Defender Offline is included in Windows 10 from the start. If you discover that there have been security breaches or that your computer is in danger, you must act immediately to guarantee your safety. In the case of a legal infraction involving your financial information, contact all banks and financial institutions with whom you have accounts. Replace the passwords on all of your services.

IX. CONCLUSIONS

Since computers and information networks permeate every aspect of our life, computer security attracts significant resources from the research network and corporate firms. No IDS will ever be able to identify every event that occurs on any specific system accurately. Modern computer architectures' increasing complexity and rapid evolution provide your complete protection. We want our intrusion detection systems to allow for a discount within a hit pc attack range.

In this paper, we analyzed materials that investigate all aspects of PC security, such as attackers and assaults, software bugs and viruses, and unique intrusion detection structures and techniques for assessing those mechanisms. The objective is to expand the analysis of security-related topics that may provide facts and quick advice to newcomers to the industry, as well as an excellent reference manual for security specialists. We also provided a thorough description of the cessations employed by one sort of type identification.

REFERENCES

[1] Bihina, M., J. Eloff, and H. Venter, January 2004.Intrusion Detection Systems: Evolution and Future Direction. Honours Thesis. The University of Pretoria, South Africa.

[2] Blomqvist, D. and J. Skantze, 1995. Intrusion Detection: A study. Technical Report Docs 95/62 Department of Computer Systems. Uppsala University.

[3] Frank, J., 1994. Artificial Intelligence and Intrusion Detection: Current and Future Directions. In Proc.17th National Computer Security Conference, National Institute of Standards and Technology. Washington, D.C.

[4] Albag, H., Retrieved October 7, 2006. Network & Agent Based Intrusion Detection Systems. Available at: www.model.in.tum.de/um/courses/seminar/worm/WS0405/albag.pdf.

[5] Velankar, A. A., Retrieved October 7, 2006. The Many Faces of Intrusion Detection System. Available at http://www.utdallas.edu/~axv028100/courses/cs6390/paper/IDS_paper_may01.pdf.

[6] Howard, J.D., 1998. An analysis of security incidents on the Internet 1989-1995, Department of Engineering and Public Policy. Carnegie Mellon University.

[7] Jones, A.K. and R.S. Sielken, 2000. Computer System Intrusion Detection: A Survey. Computer Science Technical Report. The University of Virginia.

[8] Verwoerd, T. and R. Hunt, 15 September 2002. Intrusion detection techniques and approaches. Computer Communications. 25(15): 1356-1365.

[9] Mirkovic, J., P. Reiher, 2004. Taxonomy of DDoS attack and DDoS defense mechanisms.ACM SIGCOMM Computer Communication Review, 34(2): 39 - 53.

[10] Specht, S.M. and R.B. Lee, September 2004. Distributed denial of service: taxonomies of attacks, tools and countermeasures. International Workshop on Security in Parallel and Distributed (17th ICPADS).

[11] Alvarez, G. and S. Petrovic, November 2002. Encoding Taxonomy of Web Attacks with Different-Length Vectors. Print arXiv:cs/0210026. Available at: http://arxiv.org/PS_cache/cs/pdf/0210/0210026. pdf

[12] Abbas, A., 2005. State of the Art Security Taxonomy of Internet Security: Threats and Countermeasures. Int'l Trans. Computer Science and Engineering, 19(1): 27-36.60.

[13] Bishop, M., May 1995. Taxonomy of UNIX system and network vulnerabilities. Technical Report CSE-9510, Department of Computer Science, the University of California at Davis. Kabiri, P. and A.A. Ghorbani, September 2005. Research on Intrusion Detection and Response: ASurvey. International Journal of Network Security.