Vol-08 Issue 05, May -2024 ISSN: 2456-9348
Impact Factor: 7.936

iJETRM
International Journal of Engineering Technology Research & Management

A STUDY OF NAVIGATING THE DYNAMIC TERRAIN OF SECURITY CHALLENGES AND TRENDS IN MODERN TECHNOLOGIES

Ms. Uma P
Assistant Professor, Dept. of Computer Science., New Horizon College, Kasturi Nagar, Bangalore.

ABSTRACT:
Personal information and computer networks must be protected using tools like firewalls, virus protection, and other software, but this is insufficient. Cybersecurity must be considered by information technology (IT) and Internet service providers (ISPs) to Strengthen cybersecurity and key information [1]. The goal of cyber security is to protect data and information systems (such as networking, computing systems, and cloud services, as well as software). Governments and businesses are trying to take a number of steps to automatically think of the growing issue of online crime. The prevalence of smartphone and private computing device-based cybercrime emphasizes the importance of staying current on global cybercrime developments. Many people are still concerned about cyber security, despite multiple safeguards. The paper focuses on the most recent developments in cyber security tactics and trends.

Keywords:
Cyber Security, information technology, Internet service providers

INTRODUCTION

Today, man can send and receive any type of data, such as an e-mail or an audio or video file, with the click of a button, Consider how securely his data is being transmitted or sent to the other person without any information leakage. The solution is found in cyber security. The Internet is now the fastest growing infrastructure in daily life. Many new technologies are changing the face of humanity in today's technological environment. However, because of these emerging technologies, we are unable to effectively protect our private information, and as a result, cybercrime is on the rise. Even the most cutting-edge technologies, such as cloud computing, mobile computing, net banking, and e-commerce, require a high level of security [2].

Since these technologies include some crucial information about a person, their security has turned into a top priority. Any country's security and economic well-being depend on enhancing cyber security and safeguarding vital information infrastructure. Keeping the Internet safer (and safeguarding users of the Internet) has become crucial to the creation of new technologies.

Cyber Security

Cybersecurity is the process of guarding against digital threats and preventing unwanted access to networks, devices, and data. IT (Information Technology) security, Which is intended to stop threats against network systems, apps, and other platforms, is another name for cybersecurity. It prevents or protects information, data, and other things, to put it simply [3].

Cyber Security Techniques

Cybersecurity is becoming more important due to an increase in unwanted intrusions into private data with the express purpose of stealing it to threaten or blackmail individuals for their personal information. The methods and instruments used to address cyber security issues are

Authentication:

This essential cyber security method aims to confirm the user's identity using the credentials saved in the system's security domain. Although password technology is the most popular form of governance, there are many different implementations available, such as the SIM card found in every person's cell phone. SIM cards come with distinctive ID numbers that are used to identify a specific cell phone via a secure communication channel. Stopping unauthorized parties from listening in on the authenticating message presents the biggest problem in the authentication process. It

is possible for dishonest persons to intercept a password sent through an unsecured medium and use it to pretend to be the intended user. The solution to this issue is encryption [1].

Encryption:

Encryption makes data unreadable unless an appropriate key is used to unlock it. It would take an enormous amount of time and computing power to solve difficult mathematical problems, such as factoring huge primes, in order to break an encryption. Symmetric encryption uses the same key for message encoding and decoding, and the key's security level is comparable. There could be security hazards associated with the dissemination of the key. With asymmetric encryption, the communication is encrypted with a public key and decrypted with a private key[4]. Asymmetric encryption is used by the vast majority of modern security systems to distribute keys.

Digital signatures:

Digital signatures can be created using the same mathematical procedures that are used in asymmetric encryption. A user is free to encrypt some data using a private key to verify that he has it. By possessing the public key that will validate the person's credentials, anyone can decode the same data. In essence, this procedure is the exact opposite of public key encryption and operates under the similar presumption that the authorized user only has access to the private key.

Anti-virus:

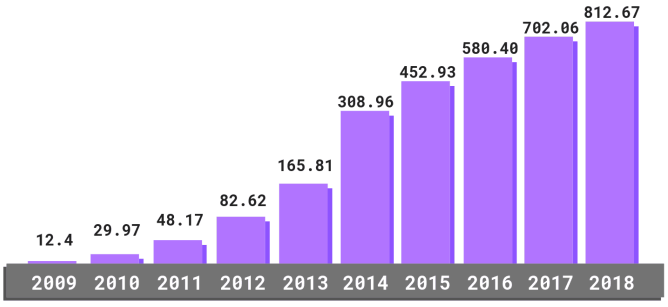
The threat of computer viruses or unwanted small programmers that execute undesired commands without the user's explicit authorization has grown to monstrous proportions [2]. Anti-virus software performs two tasks: it searches the systems for viruses that are already there and stops viruses from being installed in a system. Because Windows is the most popular computing platform among the general public, the majority of viruses have been developed to target it. Users of Apple and Linux operating systems may also be targeted by viruses created specifically for those platforms.

Firewall:

When a computer is connected to the internet directly or through other network connections, firewalls successfully thwart any attempt by hackers to gain unauthorized access to the machine. Most operating systems include a firewall and have it switched on by default. If the default firewall's security level is insufficient or it is interfering with lawful network activity, it may be necessary to use a commercial firewall [1].

Malware Scanners:

A computer programmer that occasionally checks all files and documents on the system for viruses or malicious code. In this sector, samples of dangerous software systems are typically sorted and labelled as malware by Trojan horses, worms, and viruses [2].



Recent Survey Issues on Cyber Security Trends

Malware is often regarded as the primary means by which malevolent forces might evade internet security measures. The most common type of attack that is placed onto a device without the owner's consent is called malware. like worms, Trojan horses, and viruses, Malware, such as spyware and bot executables, can infect computers in a number of methods, such as by spreading from infected devices, tricking users into opening suspicious files, or luring users to malicious websites. In more tangible instances of malware infection, malware may install itself into a USB drive entered into a compromised computer and then infect any system into which the compromised computer was

subsequently inserted. The computational logic and embedded systems of equipment and gadgets can transmit malware. The computational logic and embedded systems of gadgets and equipment can transmit malware. At any point in a device's life cycle, malware can be introduced. Malware can affect end users, servers, network devices (such as routers, switches, etc.), and even process control systems like SCADA. There is currently a lot of anxiety online about the complexity and growth of malware.

Preventive measures to avoid Cybercrimes:

E-identity protection

When disclosing private information online, such as your name, address, phone number, or financial information, exercise caution. While accessing or utilizing social networking sites, for example, check that the website is secure and that privacy settings are enabled.

Social Media Networking

Personal cyber dangers will increase as social media use increases. Both the use of social media by corporations and the potential of assault are rapidly increasing. Organizations can anticipate a rise in the usage of social media profiles as a distribution channel for social engineering techniques in 2012. Companies will need to move beyond the fundamentals of policy and process development to more cutting-edge technology like data leakage prevention, improved network monitoring, and log file analysis to battle the threats.

Protect your Wi-Fi network.

If Wi-Fi (wireless) networks are not properly secured, they are open to intrusion. Examine and change the default settings. Public Wi-Fi, popularly known as "Hot Spots," is also prone to attack. Avoid using these networks for business or financial operations [3].

Block spyware attacks

Installing and maintaining anti-spyware software will stop spyware from getting on your computer.

Protect your Data

For your most sensitive documents, such as tax returns or financial records, use encryption. Make regular backups of all of your crucial data, and store it somewhere else.

The safety of future Cybercrime cannot be detected in digital environments without the use of technological tools; legislative actions, organizational changes, and capacity building were also necessary.

Conclusion

Due to the massive growth in Internet access and the development of Internet-capable gadgets, as well as the growing population and widespread Internet use, extremely sensitive personal data is regularly shown online with little awareness of the consequences of information leaking.

We predict that as the amount of information available on the internet grows in the future, worries about end-user confidentiality will increase along with it.

Moreover, usability issues are becoming more and more important as a way to understand and utilize end-user-focused security measures without complication [1].

Because the original Internet was created in a somewhat different context from how it is utilized today, some people think this innovative technique has failed and won't be able to meet future needs. It is proposed to take a "thinking beyond" strategy to better utilize the escalating demands of the future rather than making reference to the current computing system or the future but rather to start over.

References

[1] Ravi Sharma Study of Latest Emerging Trends on Cyber Security and its challenges to Society International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012 1ISSN 2229-5518.

[2] Lee, H.; Lee, Y.; Lee, K.; Yim, K. Security Assessment on the Mouse Data using Mouse Loggers. In Proceedings of the International Conference on Broadband and Wireless Computing, Communication and Applications, Asan, Korea, 5–7 November 2016

[3] Mellado, D.; Mouratidis, H.; Fernández-Medina, E. Secure Troops Framework for Software Product Lines Requirements Engineering. Compute. Stand. Interfaces 2014, 36, 711–722.

[4] Schjolberg/Hubbard, “Harmonizing National Legal Approaches on Cybercrime”, 2005.

[5] The most Important Instruments in fight against Cybercrime, Ch. 6.2