International Research Journal of Multidisciplinary Science & Technology
www.irjmrs.com
ISSN : 2455-930X

DATA PRIVACY CHALLENGES AND ITS EMERGING TECHNOLOGIES

[1]Dr.R.DEEPA MCA.,MPhil.,Ph.D., and [2]P. NARMATHA
[1]Assistant Professor, Department Of Computer Science, Nallamuthu Gounder Mahalingam College, Pollachi, India.
Email:deepaharini2015@gmail.com
[2]Department Of Computer Science, Nallamuthu Gounder Mahalingam College, Pollachi, India.
Email:narmatha2001ctngm@gmail.com

Abstract

In the world of information technology, cyber security is crucial. One of the main problems in the modern world is information security. Cybercrimes, which are growing significantly every day, are the first thing that comes to mind when we think about cyber security. Numerous governments and businesses are taking numerous precautions to stop these cybercrimes. In spite of several precautions, many people are still quite concerned about cyber security. This essay primarily focuses on the difficulties that modern technology and effective cyber security management present.

Keywords: Data Privacy, cyber security, cyber crime, challenges and technologies.

I. INTRODUCTION

India's internet usage is expanding quickly. It has created new opportunities in every imaginable industry, including business, sports, entertainment, and education. Every coin has two sides. Cybercrime, or unlawful conduct carried out online, is one of the drawbacks of the internet. Cybersecurity is the term used to describe the technologies and procedures used to safeguard computers, networks, and data against unauthorised access, flaws, and attacks carried out by online criminals.

Cyber security standards are security norms that allow businesses to use secure procedures to reduce the amount of successful cyber attacks. Many cutting-edge technologies are altering the face of humanity in today's technological environment [1]. Because of these new technologies, we are unable to effectively protect our private information, which is why cybercrime is on the rise right now. Any country's security and economic well-being depend on enhancing cyber security and safeguarding vital information infrastructure. The growth of new services and governmental policy now depend on making the Internet safer (and protecting Internet users).

A thorough and safer strategy is required to combat cybercrime. Since that technology solutions cannot, by themselves, prevent every crime, it is essential to give law enforcement agencies the resources they need to successfully investigate and prosecute cybercrime. To prevent the loss of any crucial data, many countries and governments today have strong rules

governing cyber security. Every person needs to receive training in cyber security in order to protect themselves from the rising number of cybercrimes.

II. EMERGENCE OF COMPUTER CRIME

In 1820, the first cybercrime was officially documented. Given that the abacus, which is regarded to be the earliest form of a computer, has been around since 3500 B.C., this is not surprising. The analytical engine developed by Charles Babbage, however, marked the beginning of the modern computer era in China, Japan, and India. In 1976, spam email was transmitted across the ARPANET for the first time. Rich Skrenta, a high school student, created the EIK Cloner in 1982, which was the first virus to be installed on an Apple computer.

Types of Cyber crime

- Hacking
- Denial of service attacks (DDos)
- Virus Dissemination
- Computer vandalism
- Cyber terrorism
- Software piracy
- Social engineering

Hacking

Hacking is the process of locating security holes in computer networks or systems and using them to obtain access. Employing a password cracking technique to obtain access to a system is one example of hacking.

Denial of Service attacks

Several systems flooding the bandwidth or resources of a targeted system, typically one or more web servers, results in a distributed denial-of-service (DDoS) assault. Such an attack frequently happens when a number of hacked systems (such as a botnet) bombard the targeted system with traffic. virus transmission malicious software that integrates with other programmes. (Viral infections, worms, Trojan horses, web hacking, email bombing, etc.)

Computer Vandalism

Instead of stealing, damage or delete data. Often, maliciously changing online content is cyber or web vandalism. It entails adding, deleting, or changing rude or inappropriate content!

Cyber terrorism

Using online attacks for terrorist purposes. Terrorists who are adept at leveraging technology are employing 512-bit encryption.

Software piracy

It alludes to the illegal duplication of some legally obtained software. Most purchased software is licenced for usage by a single user or at a single computer location. In addition, when someone purchases software, they are referred to as "licenced users" rather than software owners.

Social engineering

Social engineering is the practise of persuading others to provide sensitive information. The kinds of information that these criminals are looking for can vary, but

when a person is targeted, the criminals typically try to trick you into giving them your bank or password information, or they try to gain access to your computer to covertly install malicious software that will give them access to your bank and password information as well as give them control over your computer.

III. IMPORTANCE OF CYBER SECURITY

A subset of computer security known as "internet security" is focused on protecting online transactions. Cyber security is the collection of tools, procedures, and techniques created to safeguard computers, networks, software, and data from damage, attack, and illegal access. Security in the context of computers refers to both physical and cyber security.

Cyber security is the process of securing sensitive personal and company data by preventing, detecting, and responding to internet threats. Look up the website's privacy statement before providing your name, email address, or other personal information. Install the updates as soon as you can if the vendor reduces fixes for the software operating system on your gadget. Installing them will make it impossible for attackers to profit. Choose a strong password that is challenging for hackers to decipher. Never select a password-remembering option for your computer.

IV.CYBER SECURITY TECHNIQUES

Access control and password security

User names and passwords have always been a key component of information security. This can be one of the initial cyber security measures.

Authentication of data

We must always validate the documents we get before downloading them. In other words, it should be verified that it came from a trustworthy source and that it hasn't been altered. Antivirus software installed on the devices typically authenticates these papers. A reliable anti-virus programme is therefore necessary to shield the gadgets from viruses.

Malware scanners

This is software that usually scans all the files and documents present in the system for malicious code or harmful viruses. Viruses, worms, and Trojan horses are examples of malicious software that are often grouped together and referred to as malware.

Firewalls

A firewall is a piece of hardware or software that aids in blocking hackers, viruses, and worms from trying to access your computer through the Internet. The firewall that is in place examines each message as it enters or leaves the internet, blocking those that do not adhere to the established security requirements. Hence, firewalls are crucial in the detection of malware.

Anti-virus software

A computer application known as antivirus software works to identify, stop, and take action against dangerous software programmes like viruses and worms. The majority of antivirus products have an auto-update capability that enables the programme to download profiles of fresh infections so that it can scan for them as soon as they are found. Every system must have anti-virus software as a minimum requirement.

V. IMPACT ON DATA PRIVACY AND ITS TRENDS

Some of the trends that are significantly affecting cyber security are listed below [1].

Web Servers

Web application attacks that aim to extract data or disseminate harmful code continue to pose a hazard. Via genuine web servers they have infiltrated, cybercriminals disseminate their malicious code. But, assaults that steal data pose a significant threat as well and are frequently covered by the media. We now need to put more of a focus on safeguarding web servers and web applications. Particularly effective platforms for these cybercriminals to steal data are web servers. In order to avoid becoming a victim of these scams, one must constantly use a safer browser, especially during critical transactions.

Cloud Computing and its Services

These days, cloud services are being gradually adopted by all small, medium, and large businesses. To put it another way, the earth is gradually advancing into the clouds. Due to the ability of traffic to bypass conventional points of inspection, this most recent trend poses a significant problem for cyber security. In order to prevent the loss of important data, policy controls for web applications and cloud services will also need to change as the number of applications available in the cloud increases. Even though cloud services are creating their own models, security concerns continue to be raised frequently. Although the cloud may offer tremendous benefits, it is important to remember that as the cloud develops, security problems also do.

APT's and targeted attacks

Advanced Persistent Threat (APT) is a brand-new tier of cybercrime software. For years, network security tools like web filtering and intrusion prevention systems (IPS) have been crucial in spotting such targeted attacks (mostly after the initial compromise). Network security must interact with other security services to detect assaults as attackers become more brazen and use hazier tactics. Thus, we must enhance our security measures to stop new risks from emerging in the future.

Mobile Networks

We can communicate with anyone, anywhere in the world, today. Yet security is a huge worry for these mobile networks. Nowadays, firewalls and other security measures are getting more permeable as more people use devices like tablets, phones, PCs, and other similar ones, all of which again need additional security measures in addition to those found in the programmes

being used. We must always consider how secure these mobile networks are. Added mobile networks include very susceptible to these cybercrimes, hence great caution must be used in the event of any security difficulties.

Encryption of the code

The act of encoding messages so that hackers or eavesdroppers cannot read them is known as encryption. An encryption algorithm is used in an encryption technique to transform the message or information into an unintelligible cypher text. An encryption key, which determines how the message is to be encoded, is typically used for this.

At its most basic level, encryption safeguards both the integrity and privacy of data. However, greater encryption use creates more cyber security challenges. Data being transported across networks (like the Internet, for example), mobile phones, wireless microphones, wireless intercoms, etc. is protected using encryption. So, by encrypting the code, one may determine whether there has been any information leaking.

Hence, the aforementioned are some of the developments that are altering the global landscape of cyber security.

VI. CYBER SECURITY TRENDS OF INDIA

The topic of cyber security has caught the interest of many Indian stakeholders. They include the Indian government, businesses, people, and banks, among others.

Digital India Security

Due to the fact that many internet services rely on it, the security of the digital India project is of the utmost importance. The Indian government must now provide cyber security for a digital India as a matter of necessity. Without cyber security, the majority of government initiatives would cause more problems than they would solve.

Digital Payment

A truly unsettling idea is the push towards digital payments without proper cyber protection. India's whole online banking and digital payment infrastructure is open to hacker assaults and online theft. Debit/credit cards, mobile wallets, online banking, and any other e-banking options that have been offered are all extremely vulnerable to sophisticated cyber attacks.

Ransomware

In the past, ransomware rose to the top of the list of annoyances. Attacks by ransomware would continue to rise in the future. Locking the data would be disastrous because India is becoming a data nation. As of right now, India has little defences against ransomware, which leaves companies vulnerable to lawsuits and feeling helpless when they are attacked.

Smart Cities Security

The Indian government is prepared to build smart cities there. Numerous smart cities received approval in the previous year, and this year may see the beginning of work on them..

.

IoT Security

The Internet of Things (IoT) has been well embraced in India over the past year. Interest in IoT-driven services has been expressed by numerous domestic and international parties. Of course, most of them are still simply investigating at this point because the legal aspects of technology are still unclear. IoT services, however, clearly need robust cyber security and civil liberties protection.

Cloud Computing Security

In India, the idea of cloud computing is comparatively well-liked. In truth, businesses and individuals have historically made investments in cloud computing initiatives. Several of our clients were reluctant to start a full-fledged cloud computing business, though.

Critical Infrastructure Protection

The Indian government has made suggestions that botnet and malware cleanup facilities may open soon. This is a good development because it would aid in protecting India's vital infrastructure. The Indian government has also periodically developed policies and rules to ensure the protection of protected systems and crucial infrastructure. In order to secure the critical infrastructures in India, the National Critical Information Infrastructure Protection Centre (NCIIPC) has also been active.

Healthcare Security

India requires a strong healthcare cyber security due to the growing usage of ICT in healthcare. This needs to be reinforced with sufficient privacy protections and strong data security.

Banking Security

The government needs to put in a lot of effort in the domain of banking cyber security. Digital payments and financial activities in India are susceptible to a variety of cyberattacks and crimes. Banks lack the resources necessary to combat sophisticated cybercrimes and cyberattacks.

Cyber Insurance

The surge in cybercrime and cyberattacks would result in significant growth for the cyber insurance industry. Yet, both insurance providers and insured parties need to be aware of certain technological and legal aspects of cyber liability insurance. Future developments in the field of cyber insurance could include the arrival of new businesses, startups, entrepreneurs, etc.

Blockchain

Some parties looked into using bitcoin and the blockchain. The blockchain, bitcoin, and its potential applications are also being studied by the Indian government and Reserve Bank of India (RBI). However, there are still open questions regarding bitcoin's legality in India and technological legal regulatory compliances.

VII. CYBER SECURITY MANAGEMENT

- Uninstall unnecessary software
- Maintain Backup

www.irjmrs.com

ISSN : 2455-930X

- Stay anonymous- choose genderless screen name
- Protect your personal information
    - Keep an eye out for phony email messages
    - Don't respond to email messages that ask for personal information .
    - Steer clear of fraudulent Web sites used to steal personal information
    - Pay attention to privacy policies on Web sites and in software guard your email address
- Keep your computer with latest patches and updates

  While keeping your computer up to date won't totally prevent you from assaults, it will make it much harder for hackers to access your system, block many common and automated attempts, and may even convince a less determined hacker to look for another computer that is more open to attack.

- Make sure your computer is configuring securely

Depending on who will be using the computer, the appropriate level of security and privacy must be chosen. By using the "Help" feature of your software or reading the vendor's website, you can frequently adjust security and privacy settings correctly without the need for any kind of specialised knowledge. If you feel uneasy setting it up yourself, ask someone you know and trust for help or get in touch with the provider.

- Choose strong passwords and keep them safe

The first step in keeping passwords secure and out of the wrong hands is choosing a password that is difficult to guess. Strong passwords use a combination of letters, numbers, and symbols (such as # $%!?), and they are eight characters or longer. Your login name, anything based on your personal information, including your last name, and terms from the dictionary should all be avoided as passwords. For the protection of activities like online banking, try to choose particularly robust, one-of-a-kind passwords. Don't use the same password for every online site you use, and save your passwords in a secure location.

- Protect your computer with security software

  Your antivirus software, which keeps an eye on all online activity including email and web browsing and defends you against viruses, worms, Trojan horses, and other harmful programmes, is frequently the next line of defence. Norton Antivirus and other more contemporary antivirus solutions offer protection against spyware and other potentially unwanted programmes like adware. To keep safe online, you must have security software that allows you control over applications you might not want and shields you from internet risks. Every time you connect to the Internet, your antivirus and antispyware software should be set up to automatically update. [5].

- Enhance security standards

  The industries and enterprises should upgrade the skills of their cyber security and the IT staff by training and certification as a short-term measure.As As

a short-term solution, businesses and sectors should train and certify their IT and cyber security workers to enhance their capabilities. As part of our long-term planning, we must create graduate-level cyber security courses and encourage international certification bodies to roll out various skills-based cyber security courses and practical performance-based skill assessment exams.

Businesses and industries should spend more money on cyber security and staff the department with qualified, trained specialists.

Cyber law of India

Traditional criminal behaviours including theft, fraud, deception, and mischief, all of which are punishable under the Indian Penal Code, can also be included in cybercrime. Cybercrime, to put it simply, is any illegal activity when a computer is either used as a tool or both. The Information Technology Act of 2008 addresses new age crimes that were created as a result of computer abuse.

VIII. CONCLUSION

In fact, cybercrime is receiving the attention it deserves. It won't be so readily restricted, though. In reality, it is likely that cybercrime and the hackers who perpetrate it will keep evolving and modernising in order to elude detection by law enforcement. Thus, we must have cyber security to make us safer. For decades, the IT sector has been playing catch-up with hackers and online criminals. Hence, in the near future, there will be a need for a cyber security curriculum that will instill a knowledge of cyber security in the Young people today and finally the IT industry will gain more knowledgeable, highly qualified workers, not just in the security sector but also in every other sector, boosting the communication and brain compatibility abilities of both the employees and the employers.

REFERENCES

[1] Atul M. Tonge, Suraj S. Kasture , Surbhi R. Chaudhari3, "Cyber security: challenges for society- literature review", IOSR Journal of Computer Engineering (IOSR-JCE), Volume 12, Issue 2 ,May. - Jun. 2013.

[2] G.Nikhita Reddy1, G.J. Ugander Reddy2, "A study of cyber security challenges and its emergning trends on latest technologies", 1- 6, International Journal of Engineering and Technology Volume 4 No. 1, January, 2014.

[3] Vaishnavi J. Deshpande1, Dr. Rajeshkumar Sambhe2, "Cyber Security: Strategy to Security Challenges- A Review", International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 9, March 2014.

[4] 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.

[5] "Understanding cybercrime: phenomena, challenges and legal response", September 2012, Telecommunication Development Sector, 2 – 366.

[6] IEEE Security and Privacy Magazine – IEEECS "Safety Critical Systems – Next Generation "July 2019.