IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 5.731
Volume 8, Issue 1, August 2021

Study on the Challenges of Cyber Security and the Emerging Patterns Associated with Modern Technologies

Ashish Chauhan[1], Ansari Saif[2], Gupta Amit[3]
Asst. Professor[1] and FYIT[2,3]
Uttar Bhartiya Sangh's Mahendra Pratap Sharda Prasad Singh College of Commerce & Science, Mumbai, Maharashtra

Abstract: *Cybersecurity is crucial to the information technology sector. Information security is a significant concern in the contemporary world. When considering cyber security, the first thing that comes to mind is the increasing prevalence of cybercrimes. Multiple governments and businesses are implementing a variety of measures to prevent these cybercrimes. Despite the implementation of several precautions, a significant number of individuals remain deeply apprehensive about the issue of cyber security. This essay largely addresses the challenges encountered by contemporary technology-driven cyber security. Furthermore, it highlights the latest updates on cyber security strategies, ethical considerations, and emerging trends that are reshaping the cyber security domain..*

Keywords: cybercrimes, governmental involvement, cyber security

I. INTRODUCTION

Today, individuals have the ability to transmit many forms of data, such as email, audio, or video, with ease. However, it is important to evaluate the level of security in place to ensure that the data is delivered to the intended recipient without any unauthorized access or leakage of information. The field of cybersecurity possesses the solution. The internet is currently experiencing the most rapid growth among the various components of modern infrastructure. Several cutting-edge technologies are transforming the essence of mankind in the contemporary technological era. Nevertheless, due to the advent of this novel technology, our ability to safeguard our confidential data has been compromised, leading to the current surge in cybercrime. In the present day, over 60% of all business transactions take place on the internet. Consequently, this sector requires a robust level of security to ensure the utmost dependability and transparency of these transactions. Therefore, cyber security has become a pressing issue. Cyber security encompasses other domains, including cyber space, beyond the mere safeguarding of data within the IT industry.

Even the most cutting-edge technologies, such as cloud computing, mobile computing, net banking, and e-commerce, require a high level of security. Since these technologies include some crucial information about a person, their security has turned into a top priority. Each 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. Given that technology solutions cannot, by themselves, prevent every crime, it is essential to give law enforcement authorities the resources they need to successfully investigate and prosecute cybercrime. To prevent the loss of any crucial data, many countries and governments now have strong rules governing cyber security. Every person has to receive training in cyber security to protect oneself from the rising number of cybercrimes.

II. CYBER CRIME

Any illicit action that employs a computer as its main tool for commission and theft is referred to as cybercrime. The United States Department of Justice broadens the definition of cybercrime to encompass any criminal action that keeps evidence on a computer. The growing list of cybercrimes includes offences made possible by computers, like network intrusions and the spread of computer viruses, as well as computer-based variations of already-committed offences, like identity theft, stalking, bullying, and terrorism, which have become major problems for individuals and nations.

ISSN 2581-9429 IJARSCT

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 5.731
Volume 8, Issue 1, August 2021

Cybercrime is typically understood to be any crime carried out online or utilising a computer to steal someone else's identity, sell illegal goods, stalk victims, or disrupt business using malicious software. The importance of technology in people's lives is increasing day by day, and as a result, so will the number of cybercrimes.

III. CYBER SECURITY

Data security and privacy are always the top security precautions that any firm takes. We currently live in a world where every information is stored digitally or electronically. Users can engage with friends and family in a setting where they feel secure using social networking sites. Cybercriminals will continue to target social media sites in the case of home users in order to steal personal information. A person must take all necessary security precautions during financial transactions as well as when using social networking sites.

The comparison of cyber security incidents reported to Cyber999 in Malaysia between January and June of 2012 and 2013 shown above amply illustrates the challenges to cyber security. Security measures are likewise getting more stringent as crime does. Silicon Valley Bank discovered that corporations feel cyber assaults are a severe danger to both their data and their business continuity in its poll of US technology and healthcare leaders.

Only one-third of companies are completely confident in the security of their information, and even fewer are confident in the security measures of their business partners. 98% of companies are maintaining or increasing their cyber security resources, and of those, half are doing so this year specifically to increase resources devoted to online attacks.

There will be new assaults on smartphones running the Android operating system, but they won't be widespread. Due to the fact that tablets and smartphones both use the same operating system, the same virus will eventually target them. Malware specimens for Macs would increase with time, but far more slowly than for PCs.

These are some of the anticipated developments in cyber security since Windows 8 will make it feasible for users to create programmes for practically any device (PCs, tablets, and smartphones) running the operating system.

IV. TRENDS CHANGING CYBER SECURITY

Some of the trends that are having a significant influence on cyber security are listed below.

4.1 Web servers:

The possibility of attacks against online apps to transmit harmful code or collect data still exists. The legitimate web servers that they have infiltrated are used by cybercriminals to disseminate their malicious malware. However, 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 being a victim of these scams, one must constantly use a safer browser, especially during critical transactions.

4.2 Cloud computing and its services:

These days, cloud services are being gradually adopted by all small, medium, and large businesses. In other words, the earth is gradually encroaching towards 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 apps 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 are still a major concern. Although the cloud may provide tremendous benefits, it is important to remember that as the cloud develops, security problems also emerge.

4.3 APT's and targeted attacks:

A new class of cybercrime software is called a "APT" (Advanced Persistent Threat). Web filtering and intrusion prevention systems (IPS) have been crucial in discovering such targeted attempts for years (usually after the initial penetration). Network security must connect with other security services to identify assaults as attackers become more daring and use hazier tactics. Therefore, we must enhance our security measures to stop new risks from emerging in the future.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 5.731
Volume 8, Issue 1, August 2021

4.4 Mobile Networks:

We can communicate with anyone, anywhere in the world, now. Security, however, is a very serious 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. Additionally, mobile networks are quite vulnerable to these cybercrimes, thus extreme caution must be used in the event of any security difficulties.

4.5 IPv6: New internet protocol:

The previous IPv4 protocol, which served as the foundation of both our networks in general and the Internet in general, is being replaced by the new IPv6 protocol. It takes more than simply migrating IPv4 capabilities to protect IPv6. While IPv6 is a complete replacement in terms of expanding the number of IP addresses accessible, there are some very basic modifications to the protocol that security policy must take into account. Therefore, it is always preferable to migrate to IPv6 as soon as feasible to lower the dangers associated with cybercrime.

4.6 Encryption of the code:

The act of encrypting communications (or information) 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 often used for this. At its most basic level, encryption safeguards both the integrity and privacy of data. However, greater encryption use creates additional cyber security issues. Additionally, encryption is used to secure data that is being exchanged across networks (such as the Internet, e-commerce), mobile devices, wireless microphones, wireless intercoms, etc. Therefore, by encrypting the code, one may determine whether there has been any information leaking.

Thus, the aforementioned are some of the developments that are altering the global landscape of cyber security. The major network risks are listed in Fig. -1 below.

V. ROLE OF SOCIAL MEDIA IN CYBER SECURITY

In an increasingly social and interconnected world, businesses must discover novel ways to safeguard customer information. Social media will have a significant impact on personal cyber dangers and plays a significant part in cyber security. The use of social media by employees is surging, much like the attack danger. Since the majority of them use social media or social networking sites virtually daily, it has developed into a significant platform for cybercriminals to break into personal data and steal vital information.

Companies must make sure they are equally as rapid in recognising risks, responding in real time, and preventing any type of breach in a world where we're ready to hand up our personal information. These social media platforms are used as bait by hackers to obtain the information and data they need since they are so readily attracting to users. Therefore, people must take the necessary precautions, especially while using social media, to prevent the loss of their information. At the core of the unique challenge that social media provides to businesses is the capacity of individuals to share information with an audience of millions. Social media not only allows anybody the ability to transmit information that is economically sensitive, but it also gives anyone the ability to propagate incorrect information, which may be just as harmful. One of the new threats noted in the Global Risks 2013 report is the quick spread of incorrect information via social media.

Even if social media may be used for cybercrime, businesses cannot afford to cease utilising it since it is crucial for brand awareness. Instead, they need solutions that will alert them to the problem so they can address it before any serious harm is done. However, in order to avoid hazards, businesses should be aware of this, acknowledge the significance of information analysis, particularly in social dialogues, and offer suitable security solutions. One must manage social media by utilising the appropriate technology and procedures.

Copyright to IJARSCT
www.ijarsct.co.in

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 5.731
Volume 8, Issue 1, August 2021

VI. CYBER SECURITY TECHNIQUES

6.1 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.

6.2 Authentication of data:

Before downloading, the papers we receive must always be validated, meaning they must be examined to ensure that they are not altered and have come from a trustworthy source. Antivirus software installed on the devices often authenticates these papers. A reliable anti-virus programme is therefore necessary to shield the gadgets from infections.

6.3 Malware scanners:

This programme typically checks all of the system's files and documents for hazardous viruses or malicious code. Malicious software such as viruses, worms, and Trojan horses are examples. This type of software is referred to as malware.

6.4 Firewalls:

A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet. All messages entering or leaving the internet pass through the firewall present, which examines each message and blocks those that do not meet the specified security criteria. Hence firewalls play an important role in detecting the malware.

6.5 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 need.

VII. CYBER ETHICS

The internet's code is nothing more than cyber ethics. There is a strong possibility that we will use the internet in an appropriate and secure manner if we put these cyber ethics into practise. Several of them are listed below:

DON'T be afraid to engage and converse with others online. It's simple to remain in touch with friends and family, talk to coworkers, and exchange ideas and information with individuals nearby or halfway around the world thanks to email and instant messaging.

Avoid bullying others online. Do not insult somebody, make false statements about them, transmit humiliating images of them, or engage in any other behaviour intended to do them harm.

The Internet is regarded as the world's biggest library, offering knowledge on any subject imaginable. As a result, it is always crucial to use this material responsibly and legally.

Do not use someone else's password to access their accounts.

Never attempt to corrupt someone else's computers by sending malware to them.

Never give out your personal information to anyone since there's a potential that someone will misuse it and get you into trouble.

When you're online, don't try to impersonate others or establish false profiles for them since doing so might get you and the other person into problems.

Always follow any copyrighted information, and only download legal games or films.

The aforementioned are a few cyber-ethics that one should adhere to when utilising the internet. From a very young age, we have always been taught the importance of following the law, and the same is true in cyberspace.

Copyright to IJARSCT
www.ijarsct.co.in

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 5.731
Volume 8, Issue 1, August 2021

VIII. CONCLUSION

Given that networks are utilized for conducting critical operations, computer security is a substantial concern that is growing in importance as global interconnectivity increases. As each year passes, cybercrime evolves and the security of information also changes. Enterprises are being challenged by the latest and most advanced technologies in terms of protecting their infrastructure. They require new platforms and intelligence to effectively defend their systems, in addition to addressing the emerging cyber tools and threats that arise on a daily basis. The eradication of cybercrimes is an unattainable goal, but it is imperative that we exert maximum effort to mitigate them in order to ensure a safe and secure future in the digital realm.

REFERENCES

[1]. A Sophos Article 04. 12v1.dNA, eight trends changing network security by James Lyne.
[2]. Cyber Security: Understanding Cyber Crimes- Sunit Belapure Nina Godbole
[3]. Computer Security Practices in Non-Profit Organisations – A NetAction Report by Audrie Krause.
[4]. A Look back on Cyber Security 2012 by Luis corrons – Panda Labs.
[5]. International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013 Page nos.68 – 71 ISSN 2229-5518, "Study of Cloud Computing in HealthCare Industry " byG.Nikhita Reddy, G.J.Ugander Reddy
[6]. IEEE Security and Privacy Magazine – IEEECS "Safety Critical Systems – Next Generation "July/ Aug 2013.
[7]. CIO Asia, September 3rd , H1 2013: Cyber security in malasia by Avanthi Kumar.