International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 06 | June - 2022 Impact Factor: 7.185 ISSN: 2582-3930

CYBER SECURITY CHALLENGES AND ITS EMERGNING TRENDS ON LATEST TECHNOLOGIES

Laxmi Bangari Naik[1], Dr. Vibha M B[2]

[1]Student, [2]Associate Professor,
Department of MCA, Dayananda Sagar College of Engineering, Bengaluru, Karnataka, India

ABSTRACT

Cyber security is very important for information and communication technology. Securing the private information and privacy of a user is becoming challenging in today's world. In the current world, it is crucial to know what cyber security is and how it can be used effectively. Now a days, important files, data, and other important virtual documents are at high risk. So, they are in need of security and protection. With better and enhanced cyber security techniques we can protect our device and data effectively. Cyber security is important because military, government, financial, medical and corporate organizations accumulate large quantities of data on their PCs and other devices.

This paper mainly focuses on challenges faced by cyber security on the latest technologies.

KEYWORDS: cyber security, cyber-crime, cyber ethics, social media, cloud computing, android apps

1.INTRODUCTION

Today's man may send and receive any type of data, whether it's an e-mail, an audio or video file, with the press of a button, but has he ever considered how securely his data is being sent or sent to the other person without any information being leaked. Cyber security is the best answer for this question. In today's world, the Internet is the fastest-growing infrastructure. Many new technologies are transforming the face of humanity in today's technological environment. However, because of this new technology, we are unable to protect our personal information as effectively as we would like, and as a result, cybercrime is on the rise. Because more than 60% of total commercial transactions are now done online, this field necessitated a high level of security for transparent and best transactions. As a result, cyber security has emerged as a hot topic. The scope of cyber security extends beyond securing information in the IT industry to various other fields such as cyber space, etc. [1] [2].

Even cutting-edge technologies such as cloud computing, mobile computing, E-commerce, and net banking necessitate a high level of security. Because these technologies contain sensitive information about a person, their security has become critical. Improving cyber security and safeguarding critical information infrastructure is critical to each country's security and economic well-being. Making the Internet safer (and protecting Internet users) has become an essential component of both the development of new services and government policy. The fight against cybercrime requires a more comprehensive and secure approach. Given that technical measures alone cannot prevent any crime, it is critical that law enforcement agencies have the ability to effectively investigate and prosecute cybercrime. Many nations and governments are now enforcing stringent cyber security laws in order to prevent the loss of critical information. Every individual must be trained in cyber security in order to protect themselves from the growing number of cyber-crimes [1].

2. CYBERCRIME

Any illegal activity that uses a computer as its primary means of commission and theft is referred to as cybercrime. The United States Department of Justice broadens the definition of cybercrime to include any illegal activity that makes use of a computer to store evidence. The growing list of cyber-crimes includes crimes made possible by computers, such as network intrusions and the spread of computer viruses, as well as computer-based variations of existing crimes, such as identity theft, stalking, bullying, and terrorism, all of which have become major issues for individuals and nations [2].

In simpler terms, cybercrime is defined as a crime committed by using a computer and the internet to steal a person's identity, sell contraband, stalk victims, or disrupt operations with malicious software. As technology

continues to play an increasingly important role in people's lives, cybercrime will rise in tandem **[3]**.

3. CYBER SECURITY

Data privacy and security will always be top security priorities for any organization. We currently live in a world where all information is stored digitally or in cyberspace. Social networking sites provide a safe environment for users to interact with friends and family. Cybercriminals would continue to target social media sites to steal personal data from home users. Not only during social networking, but also during bank transactions, a person must take all necessary security precautions [2].

Incidents	Jan-June 2012	Jan-June 2013	% Increase/ (decrease)
Fraud	2439	2490	2
Intrusion	2203	1726	(22)
Spam	291	614	111
Malicious code	353	442	25
Cyber Harassment	173	233	35
Content related	10	42	320
Intrusion Attempts	55	24	(56)
Denial of services	12	10	(17)
Vulnerability reports	45	11	(76)
Total	5581	5592	

Table I

The comparison of Cyber Security Incidents reported to Cyber999 in Malaysia between January–June 2012 and 2013 clearly demonstrates cyber security threats [1] [4]. Security measures are increasing in tandem with the rise in crime. According to Silicon Valley Bank's nationwide survey of technology and healthcare executives, companies believe cyber-attacks pose a serious threat to both their data and their business continuity.

• 98 percent of businesses are maintaining or increasing their cyber security resources this year, with half increasing resources devoted to online attacks.

• The majority of businesses are preparing for cyber-attacks when they occur rather than if they occur.

• Only one-third are completely confident in the security of their information and even less confident in the security measures of their business partners. There will be new attacks on Android-based devices, but they will be limited in scope. Because tablets and smartphones use the same operating system, they will soon be targeted by the same malware. The number of malware specimens for Macs would continue to rise, though much more slowly than for PCs.

Because Windows 8 will allow users to develop applications for virtually any device (PCs, tablets, and smartphones) running Windows 8, malicious applications similar to those for Android will be possible; thus, these are some of the predicted trends in cyber security [2].

4. TRENDS CHANGING CYBER SECURITY

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

4.1 Web servers

The threat of web application attacks to extract data or distribute malicious code remains. Cybercriminals distribute malicious code through legitimate web servers that they have compromised. However, data-stealing attacks, many of which garner media attention, pose a significant threat. We must now place a greater emphasis on safeguarding web servers and web applications. Web servers are the ideal platform for these cyber criminals to steal data. As a result, in order to avoid becoming a victim of these crimes, one should always use a safer browser, especially during important transactions [4].

4.2 Cloud computing and its services

Cloud services are being gradually adopted by all small, medium, and large businesses these days. In other words, the world is gradually approaching the clouds. This latest trend poses a

significant challenge for cyber security because traffic can bypass traditional points of inspection. Furthermore, as the number of cloud-based applications grows, policy controls for web applications and cloud services will need to evolve in order to prevent the loss of valuable data. Even though cloud services are developing their own models, many concerns have been raised about their security. Although the cloud offers numerous advantages, it should be used with caution. It should be noted that as the cloud evolves, so do the security concerns [4].

4.3 APT's and targeted attacks

Advanced Persistent Threats and Targeted Attacks APT (Advanced Persistent Threat) is a completely new level of cybercrime software. For many years, network security capabilities such as web filtering and intrusion prevention systems (IPS) have been critical in detecting such targeted attacks (mostly after the initial compromise). As attackers become more daring and use more evasive techniques, network security must integrate with other security services to detect attacks. As a result, we must improve our security techniques in order to prevent future threats [4].

4.4 Mobile Networks

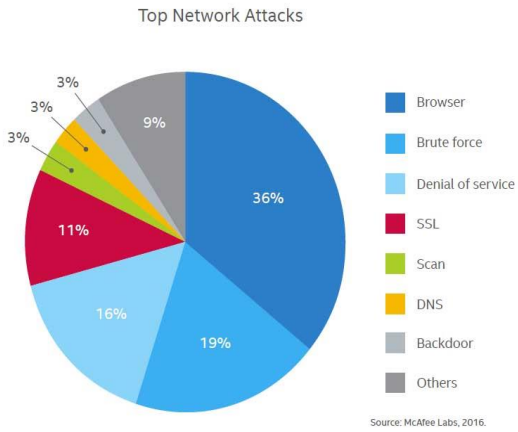
Today, we can communicate with anyone, anywhere in the world. However, security is a major concern for these mobile networks. Firewalls and other security measures are becoming more porous as people use devices such as tablets, phones, PCs, and so on, all of which require additional safeguards in addition to those provided by the applications used. We must always consider the security of these mobile networks. Furthermore, because mobile networks are so vulnerable to cybercrime, extreme caution must be taken in order to prevent them [1] [4].

4.5 IPv6:

IPv6 is the new Internet protocol that is replacing IPv4 (the older version), which has been the backbone of the Internet. It is not enough to simply port IPv4 capabilities to protect IPv6. While IPv6 is a complete replacement in terms of increasing the number of available IP addresses, there are some fundamental changes to the protocol that must be considered in security policy. As a result, it is always preferable to switch to IPv6 as soon as possible in order to reduce the risks associated with cybercrime [5].

4.6 Encryption of the code

Encryption is the process of encoding messages (or information) in such a way that it cannot be read by hackers. An encryption scheme, encrypts a message or information using an encryption algorithm, resulting in unreadable text. This is typically accomplished through the use of an encryption key, which specifies how the message should be encoded. Encryption protects data privacy and integrity from the start. However, increased encryption use creates new challenges in cyber security. Encryption is also used to protect data in transit, such as data transferred over networks (such as the Internet or ecommerce), mobile phones, wireless microphones, wireless intercoms, and so on. The are mentioned in below Fig -1. F



The above pie chart shows about the major threats for networks and cyber security [4] [6].

5 ROLE OF SOCIAL MEDIA IN CYBER SECURITY

Companies must find new ways to protect personal information as we become more social in an increasingly connected world. Social media plays a significant role in cyber security and will significantly contribute to personal cyber threats. The use of social media among personnel is increasing, as is the threat of an attack. Because most people use social media or social networking

sites every day, it has become a huge platform for cyber criminals to hack private information and steal valuable data. Companies must ensure that they are just as quick in identifying threats, responding in real time, and avoiding any kind of breach in a world where we are quick to give up our personal information. Because people are easily drawn to these social media platforms, hackers use them as bait to obtain the information and data they require. As a result, people must take appropriate precautions, particularly when dealing with social media, to avoid data loss. Individuals' ability to share information with an audience of millions is at the heart of the unique challenge that social media presents to businesses. In addition to granting anyone the ability to disseminate commercially sensitive information, social media also grants the same ability to disseminate false information, which can be equally damaging. One of the emerging risks identified in the Global Risks 2013 report is the rapid spread of false information via social media.

Though social media can be used for cybercrime, these companies cannot afford to stop using it because it is important for company publicity. Instead, they need solutions that will alert them to the threat so that they can fix it before any real damage is done. Companies, on the other hand, should understand this and recognize the importance of analyzing information, particularly in social conversations, and provide appropriate security solutions to avoid risks. Certain policies and technologies must be used to manage social media [1] [2].

6. CYBER SECURITY TECHNIQUES

6.1 Access control and password security

The concept of a user name and password has been a fundamental method of protecting our data. This could be one of the first cyber security measures. 6.2 Data authentication

6.2 Authentication of data

Before downloading, the documents we receive must always be authenticated, which means they must have come from a trusted and reliable source and have not been altered. The anti-virus software installed on the devices typically authenticates these documents. As a result, good anti-virus software is also required to protect the devices from viruses [2].

6.3 Malware scanners

This is software that scans all of the files and documents in the system for malicious code or viruses. Malicious software such as viruses, worms, and Trojan horses is commonly grouped together and referred to as malware [2].

6.4 Firewalls

A firewall is a piece of software or hardware that helps to filter out hackers, viruses, and worms that try to connect to your computer via the Internet. All messages entering or leaving the internet are routed through the firewall, which inspects each message and blocks those that do not meet the specified security criteria. As a result, firewalls are critical in detecting malware [2].

6.5 Anti-virus software

Antivirus software is a computer program that detects, prevents, and responds to malicious software programs such as viruses and worms. Most antivirus programs include an auto-update feature that allows the programmer to download virus profiles as they are discovered, allowing it to check for new viruses as soon as they are discovered. Anti-virus software is a must and a basic requirement for any system [2].

7. CYBER ETHICS

Cyberethics are simply the rules of the internet. When we practice this cyberethics, we have a better chance of using the internet properly and safely.

Here are a few examples:

- DO make use of the Internet to communicate and interact with others. Email and instant messaging make it simple to communicate with friends and family, stay in touch with coworkers, and share ideas and information with people across town or halfway around the world. On the Internet, don't be a bully.
- Do not call people names, tell lies about them, send them embarrassing pictures, or do anything else to hurt them.
- Because the Internet is regarded as the world's largest library, containing information on any topic in any subject area, using this information in a correct and legal manner is always essential.
- Do not use other people's passwords to access

their accounts.

- Never attempt to corrupt other people's systems by sending malware.
- Never give out your personal information to anyone because there is a good chance that others will misuse it and you will end up in trouble.
- When you're online, never pretend to the other person, and never try to create fake accounts on someone else's behalf because it will get you and the other person in trouble.
- Always respect copyrighted information and only download games or videos if they are legal. The following are some cyber ethics to keep in mind when using the internet. We have always thought about proper rules from the beginning, and the same is true in cyberspace [7].

CONCLUSION

Cyber security is a broad topic that is becoming increasingly important as the world becomes more interconnected, with networks used to carry out critical transactions. With each New Year that passes, cybercrime continues to take different paths, as does information security. The most recent and disruptive technologies, as well as new cyber tools and threats that emerge on a daily basis, are presenting organizations with new challenges in terms of not only securing their infrastructure but also requiring new platforms and intelligence to do so. There is no perfect solution to cybercrime, but we should do everything possible to reduce them in order to have a safe and secure future in cyberspace.

References

[1] S. K. G and M. R. M. J, "Cyber SecurityChallenges and Latest Technology Used," *International Journal of Recent Trends in Engineering & Research (IJRTER)*, vol. 2, no. 12, pp. 2455-1457 , December - 2016.

[2] H. Iqbal, . G. Al-Utaibi and O. P. Bohra, "The Reality of Technologies for Cyber Security Challenges," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 9, no. 1, April 2020.

[3] L. corrons, in *A Look back on Cyber Security*, Panda Labs, 2012 .

[4] D. o. T. S. James Lyne, "Eight Trends That Are Changing Network Security".

[5] "Top 7 Network Attack Types in 2016," Calyptix, 13 June 2016. [Online]. Available: https://www.calyptix.com/research/top-7-network-attack-types-2016/.

[6] S. Kumar and A. Singh, "Cyber Security Challenges and Its Emerging Trends on Cloud Security Issues and Techniques," *Ignited Minds Journals*, vol. 16 / Issue: 4, no. Mar, 2019, pp. 1409 - 1412 (4), Mar, 2019.

[7] T. D. Z. b. Y. and . L. C. M. b. A. (. C. , "PayWave Malaysia Threat Landscape 2018 – Based on Incidents Reported to CyberSecurity," 2019. [Online]. Available: https://www.cybersecurity.my/data/content_files/12/1971.pdf.

[8] S. B. N. Godbole, Wiley India Pvt Ltd, 2011, p. 636.