International Journal of Advanced Computational Engineering and Networking, ISSN(p): 2320-2106, ISSN(e): 2321-2063
Volume-9, Issue-5, May.-2021, http://iraj.in

A STUDY ON CHALLENGES IN CYBER SECURITY DURING PANDEMICAND ITS EMERGNING TRENDS ON LATEST TECHNOLOGIES

[1]NEERU MALIK, [2]BINDU SAINI

[1]Innovative Lab Incharge, S.B.Patil Public School, Pune, India
[2]Principal, S.B.Patil Public School, Pune, India
E-mail: neeru1508@gmail.com

Abstract - Cyber Security plays an important role in the field of information and technology. Security of the information have become one of the biggest challenges in the present day. Various companies and Governments are taking many measures in order to prevent these cyber-crimes. Whenever we think about the cyber security the first thing that comes to our mind is 'cyber crimes' which are increasing a lot day by day. Besides various measures cyber security is still a very big concern to many companies. This paper mainly focuses on challenges faced by cyber security on the latest technologies during this COVID-19 pandemic time. It also focuses on latest about the cyber security ethics, techniques, and the trends changing the face of cybersecurity.

Keywords - Cyber security, cyber ethics, cyber-crime, cloud computing, social media and android apps.

I. INTRODUCTION

The internet was born around 1960's where its access was limited to few scientists, researchers and the defence only. Internet user base have evolved expontinanlty. Initially the computer crime was only confined to making a physical damage to the computer and related infrastructure. Around 1980's the trend changed from physical damage to computers to make a computer malfunction using a malicious code called virus. Till then the effect was not so widespread because internet was only restricted to large international companies and defence sector, and research communities. In 1997, when internet was launched for the common people, it immediately became popular among the people and they slowly became dependent on it to an extent that it has changed their lifestyle. The GUIs were written so well that the user doesn't have to bother how the internet was functioning. They have to simply make few click over the hyperlinks or type the desired information at the desired place without bothering where this data is stored and how it is sent over the internet or whether the data can accessed by another person who is connected to the internet or whether the data packet sent over the internet can be snoofed and tempered. The focus of the computer crime shifted from merely damaging the computer or destroying or manipulating data for personal benefit to financial crime. These computer attacks are increasing at a rapid pace. Every second around 25 computers became victim to cyber-attack and around 800 million individuals are affected by it till 2013. CERT-India have reported around 308371 Indian websites to be hacked between 2011-2013. It is also estimated that around $160 million are lost per year due to cyber-crime. This figure is very conservative as most of the cases are never reported. According to the 2013-14 report of the standing committee on Information Technology to the 15th Lok Sabha by ministry of communication and information technology, India is a third largest number do Internet users throughout the world with an estimated 100 million internet users as on June, 2011 and the numbers are growing rapidly. There are around 22 million broadband connections in India till date operated by around 134 major Internet Service Providers (ISPs). Before discussing the matter further, let us know what the cyber-crime is? The term cyber-crime is used to describe an unlawful activity in which computer or computing devices such as smartphones, tablets, Personal Digital Assistants (PDAs), etc. which are stand alone or a part of a network are used as a tool or/and target of criminal activity. It is often The internet was born around 1960's where its access was limited to few researchers, scientists and the defence sector only. Internet user base have evolved exponentially. Initially the computer crime was only confined up to a physical damage to the computer and related infrastructure. Around 1980's the trend changed from causing the physical damaging to computers to making a computer malfunction using a malicious code called virus. Till then the effect was not so widespread because internet was only confined to defence setups, large international companies and research communities. In 1996, when internet was launched for the public, it immediately became popular among the masses and they slowly became dependent on it to an extent that it have changed their lifestyle.

II. CYBERCRIME

The term cyber-crime is used to describe an unlawful activity in which computer or some computing devices such as tablets, smart phones, Personal Digital Assistants (PDAs), etc. which alone or a part

of a network are used as a tool or target of some criminal activity or Cyber-crime is a term used for some illegal activity which uses a computer as its primary means of theft and commission. The list of cyber-crimes includes crimes that have been made possible with the help of computers, such as dissemination of computer viruses and network intrusions, as well as computer-based variations of existing crimes, such as identity theft, stalking, bullying and terrorism which have become a major problem to people and nations. Usually in layman language cyber-crime may be defined as crime committed by using a computer and the internet to steel a person's identity or some official data of a company. In 21st century technology is playing a major role in a person's life so the cyber-crimes will also increase along with the advance in the technologies.

III. CYBERSECURITY

Privacy and security of the data will always be the top concern of any organization. We are presently living in a world where all the information is maintained in a digital form specially during this pandemic time. Social networking sites is a place where users feel safe as they interact with friends and family. These days school and college education is also going online. In the case of home users, cyber-criminals would target social media sites to steal personal data of the user. Not only social networking but also while doing the bank transactions a person must take all the required security measures. Technology and healthcare executives all over the world, found that companies believe cyber-attacks are a serious threat to both their official data and their businesscommunity.

- The majority of companies are preparing for whencyber-attacksoccur
- 98% of companies are maintaining or increasing their cyber security resources and of those, half are increasing resources devoted to online attacks thisyear
- Only one-third are completely confident in the security of their information and even less confident about the security measures of their businesspartners.

As in the year 2020 the impact of COVID-19 was very extreme. This year all the work done in offices are online, due to which the cyber security is at very high risk. Some of the difficulties faced during 2020 year is listed below:-

- Hacker leaks data of 18companies

Impact- Records of 386 million users stolen from 18 companies.

- ExperianBreach

Impact: Records of 24 million people and 793,749 businesses' data stolen.

- MGMHotel

Impact- Details of over 10.6 million users revealed.

- Cognizant Technology SolutionsCorp

Impact: Disruption of client services, revenue and impact on margins. The company paid $50-70 M for ransom.

- CaliforniaUniversity

Impact: A ransom of $1.14M paid.

- World Health Organisation(WHO)

Impact: 25,000 email addresses and passwords stolen.

- Energias de Portugal(EDP)

Impact: 11 TB data stolen, and $10.8 M demanded.

- ZoomApp

Impact: Reputation and brand image damaged.

- MitsubishiElectric

Impact: 200 MB files stolen.

There will be new attacks on Android operating system based devices, but it will not be on a very large scale. The fact tablets share the same operating system as smart phones means they will be soon targeted by the same malware as those platforms.

The number of malware specimens for Macs would continue to grow, though much less than in the case of PCs. Windows 8 will allow users to develop applications for virtually any device (PCs, tablets and smart phones) running Windows 8, so it will be possible to develop malicious applications like those for Android, hence these are some of the predicted trends in cyber security.

IV. TRENDS CHANGING CYBERSECURITY

Here mentioned below are some of the trends that are having a huge impact on cyber security.

4.1. Cloud computing and its services

These days all small, medium and large companies are slowly adopting cloud services. In other words the world is slowly moving towards the clouds. This latest trend presents a big challenge for cyber security, as traffic can go around traditional points of inspection. Additionally, as the number of applications available in the cloud grows, policy controls for web applications and cloud services will also need to evolve in order to prevent the loss of valuable information. Though cloud services are developing their own models still a lot of issues are being brought up about their security. Cloud may provide immense opportunities but it should always be noted that as the cloud evolves so as its security concerns increase.

4.2. Webservers

The threat of attacks on web applications to extract data or to distribute malicious code persists. Cyber criminals distribute their malicious code via legitimate web servers they've compromised. But data-stealing attacks, many of which get the attention

of media, are also a big threat. Now, we need a greater emphasis on protecting web servers and web applications. Web servers are especially the best platform for these cyber criminals to steal the data. Hence one must always use a safer browser especially during important transactions in order not to fall as a prey for thesecrimes.

4.3. Mobile Networks

Today we are able to connect to anyone in any part of the world. But for these mobile networks security is a very big concern. These days firewalls and other security measures are becoming porous as people are using devices such as tablets, phones, PC's etc all of which again require extra securities apart from those present in the applications used. We must always think about the security issues of these mobile networks. Further mobile networks are highly prone to these cyber crimes a lot of care must be taken in case of their security issues.

4.4. APT's and targetedattacks

APT (Advanced Persistent Threat) is a whole new level of cyber crime ware. For years network security capabilities such as web filtering or IPS have played a key part in identifying such targeted attacks (mostly after the initial compromise). As attackers grow bolder and employ more vague techniques, network security must integrate with other security services in order to detect attacks. Hence one must improve our security techniques in order to prevent more threats coming in the future.

4.5. Encryption of the code

Encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it.. In an encryption scheme, the message or information is encrypted using an encryption algorithm, turning it into an unreadable cipher text. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Encryption at a very beginning level protects data privacy and its integrity. But more use of encryption brings more challenges in cyber security. Encryption is also used to protect data in transit, for example data being transferred via networks (e.g. the Internet, e-commerce),mobile

4.6. IPv6: New internet protocol

IPv6 is the new Internet protocol which is replacing IPv4 (the older version), which has been a backbone of our networks in general and the Internet at large. Protecting IPv6 is not just a question of porting IPv4 capabilities. While IPv6 is a wholesale replacement in making more IP addresses available, there are some very fundamental changes to the protocol which need to be considered in security policy. Hence it is always better to switch to IPv6 as soon as possible in order to reduce the risks regarding cyber crime.

Hence the above are some of the trends changing the face of cyber security in the world. The top network threats are mentioned in below Fig -1.

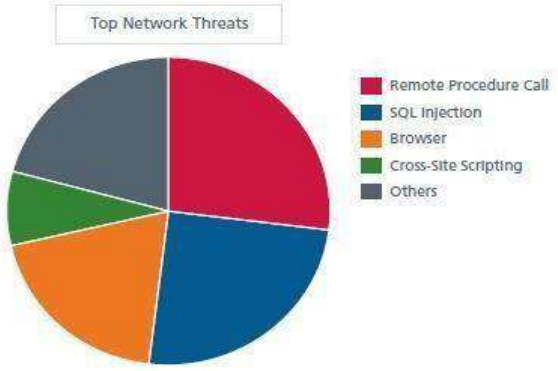

Fig -1 - The above pie chart shows about the major threats for cybersecurity and networks.

V. ROLE OF SOCIAL MEDIA IN CYBERSECURITY

The main purpose of social networking sites is to connect people and organizations. It has also developed many business opportunities for companies and firms. Social media has introduces significant change in the way people communicate. Social networking sites bring out a specific concern related to privacy and security of the user. The security and privacy of these sites mainly focuses on malware detection as it appears to come from a trusted contact, users are more likely to click on the link. The social networking sites have formed applications in many areas like-

Social e-commerce: The social networking sites can be used for the promotions and advertisements for e-commerce portal owners.

Branding: The social media provides a better platform to the companies to attract customers for more business opportunities. The ability of individuals to share information with an audience of millions is at the heart of the particular challenge that social media presents to businesses. In addition to giving anyone the power to disseminate commercially sensitive information, social media also gives the same power to spread false information, which can be just being as damaging. The rapid spread of false information through social media is among the emerging risks identified in Global Risks 2015 report. Though social media can be used for cyber crimes these companies cannot afford to stop using social media as it plays an important role in publicity of a company. Instead, they must have solutions that will notify them of the threat in order to fix it before any real damage is done. However companies should understand this and recognise the importance of analysing the information especially in social conversations and provide appropriate security solutions in order to stay away from risks. One must handle social media by using certain policies and righttechnologies.

es, wireless micro

VI. CYBER SECURITY TECHNIQUES

6.1. Access control and password security

The concept of user name and password has been fundamental way of protecting our information. This may be one of the first measures regarding cyber security.

6.2. 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.

6.3. Authentication of data

The documents that we receive must always be authenticated be before downloading that is it should be checked if it has originated from a trusted and a reliable source and that they are not altered. Authenticating of these documents is usually done by the anti virus software present in the devices. Thus a good anti virus software is also essential to protect the devices from viruses.

6.4. Anti-virussoftware

Antivirus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software programs, such as viruses and worms. Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered. An anti virus software is a must and basic necessity for every system.

6.5. 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.

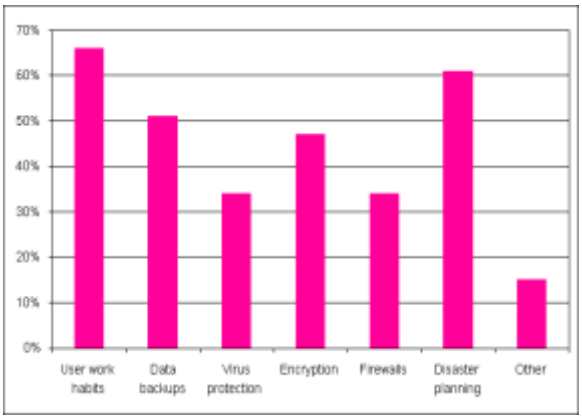

Table II: Techniques on cyber security

VII. CYBER ETHICS

Cyber ethics are nothing but the code of the internet. When we practice these cyber ethics there are good chances of us using the internet in a proper and safer way. The below are a few of them:

- Don't be a bully on the Internet. Do not call people names, lie about them, send embarrassing pictures of them, or do anything else to try to hurt them.
- Do not operate others accounts using their passwords.
- Never share your personal information to anyone as there is a good chance of others misusing it and finally you would end up in atrouble.
- DO use the Internet to communicate and interact with other people. Email and instant messaging make it easy to stay in touch with friends and family members, communicate with work colleagues, and share ideas and information with people across town or halfway around theworld
- Internet is considered as world's largest library with information on any topic in any subject area, so using this information in a correct and legal way is always essential.
- Always adhere to copyrighted information and download games or videos only if they are permissible.
- Never try to send any kind of malware to other's systems and make them corrupt.
- When you're online never pretend to the other person, and never try to create fake accounts on someone else as it would land you as well as the other person into trouble.

The above are a few cyber ethics one must follow while using the internet. We are always thought proper rules from out very early stages the same here we apply in cyber space.

VIII. CONCLUSION

Computer security is a very big topic that is becoming more important in this 21st century because the world is becoming highly interconnected, with networks being used to carry out critical transactions. And during this pandemic time also everything was digitalized. Cyber-crime continues to expand down different paths every year and so does the security of the information is also hampered. The disruptive and the latest technologies, along with the new cyber tools and threats that come to light each day, are challenging organizations with not only how they secure their infrastructure, but how they require new platforms and intelligence to do so. There is no exact solution for these cyber-crimes but we can try our level best to minimize them in order to have a secure and safe future in cyber space.

REFERENCE

[1] A Sophos Article 04.12v1.dNA, eight trends changing network security by JamesLyne.
[2] Cyber Security: Understanding Cyber Crimes- Sunit Belapure NinaGodbole
[3] Computer Security Practices in Non Profit Organisations – A NetAction Report by Audrie Krause.
[4] A Look back on Cyber Security 2015 by Luis corrons – PandaLabs.
[5] International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September- 2016 Page nos.68 – 71 ISSN 2229-5518, "Study of Cloud Computing in healthCare industry " by G.Nikhita Reddy, G.J.UganderReddy
[6] IEEE Security and Privacy Magazine – IEEECS "Safety Critical Systems – Next Generation "July/ Aug2017.

★★★