IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CYBERCRIME AND OTHER CYBERSECURITY CHALLENGES ON LATEST TECHNOLOGIES

Swapnil Yashwant Dhanawde
Department of Information Technology
University of Mumbai, Fort, Mumbai

***Abstract*—Cyber Security is very important concept of Information technology. As data is considered very important asset in today's world and biggest challenge is to secure this data and now days rate of cybercrime is getting increased day by day, various government agencies are taking measures to prevent this crime. This paper mainly focuses on challenges faced by cyber security on latest technologies and techniques, ethics and trends changing the face of cyber security.**

Keywords—cyber security, cybercrime, social media, cloud, android apps.

I. INTRODUCTION

Everyone is able to send and receive data on e-mail or any other social media platform by just on a single click, we don't even think that how securely the data is been transmitted over the internet and did it is been received by the correct recipient without any leakage. Cyber security comes in the scenario while protecting our data in this transmission. Internet is a vast and emerging infrastructure which is very crucial after this pandemic situation where most of people are working from home and most of businesses are turned digital. Due to this situation, it is very important to safeguard our private information in an effective way but due to increase in use of internet it is becoming difficult to protect any kind of leakages and cybercrimes. After the introduction of UPI payments, over 60-70% of transactions are done online both for commercial and personal purposes, so this requires high quality of security for fast and secure transaction. The scope of cyber security is not just limited to the IT industry but it is extended to other fields like banking sector, cyber space etc.

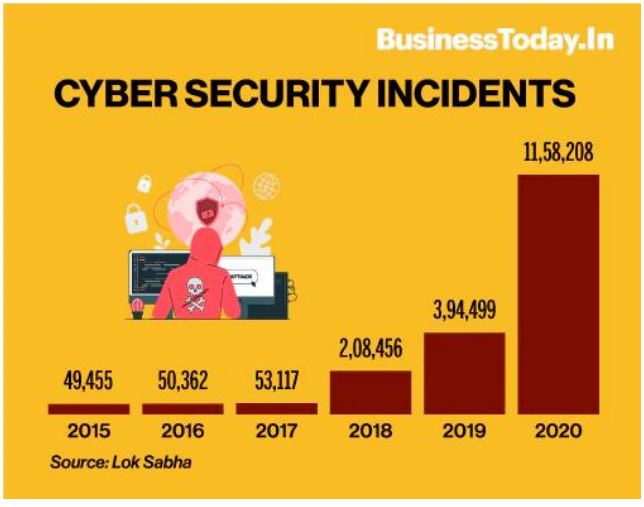
Even technologies like cloud computing, mobile networks, E-commerce etc. also required high level of security. Since these technologies required huge amount of personal information of their customers and other parties it must be protected from any unwanted attack. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic wellbeing. Protecting internet users and making internet safer has become integral to develop new government policies to fight against cybercrimes. Fight against cybercrimes needs a comprehensive approach such that not only technical measures alone cannot prevent any crime, it has become critical that law enforcement agencies are allowed to investigate the cybercrime effectively. Today many nations and governments are imposing strict laws on cyber securities in order to prevent the loss of some important information. Every individual must also be trained on this cyber security and save themselves from these increasing cybercrimes.

II. CYBER CRIMES

Cybercrime is an illegal activity that uses the computer as it's primary means of commission and theft. U.S. Department of Justice defines that cybercrime to include any illegal activity uses a computer for storage of evidence. The emerging list of cybercrime includes the attacks that have possibly made by computers, such as network intrusion and dissemination of computer viruses, also any computer-based variation of existing crimes such as identity theft, stalking, bullying and terrorism. In common man's terms cybercrime is a crime that is been committed using a computer and internet to steal a person's identity or sell contraband or stalk victims. Day by day technology and internet is playing a major role in a person's life with this growing dependency cybercrimes are also to be increase along with this.

III. CYBER SECURITY

Security and Privacy of data will always be top security measures of any organization take care of. Presently we are living in world where all the information is maintained in digital format, social networking sites provides user platform to feel safe as they interact with their friends and family. In the case of home users, cyber-criminals would continue to target social media sites to steal personal data. Not only social networking also bank transactions requires security measures



As per above image, is the comparison of cyber security incidents which took placed in past 6 years as we can clearly see that due to most of businesses and social media moving towards digitization cyber security incidents are also getting increased. Most of big companies are now started investing more in security measures in order to protect their and customers data which is very sensitive and crucial for business continuity. Most recent incident was occurred with the Jubilant FoodWorks which runs the chain Dominos Indian outlet, in this attack customer data like name, e-mail id. Mobile number, GPS location were leaked through Dark Web. Data of over 18 Crore orders of Domino's India became public.

IV. TRENDS CHANGING CYBER SECURITY

Below are some changes that are having a huge impact on cyber security

A) Web servers:

The threat of cyber-attacks on web applications to extract data or to distribute malicious code persists. Cyber criminals distribute their malicious code via permissible web servers they have compromised. Data-stealing attacks, many of which get the attention of media, are also a big threat. We need a greater emphasis on protecting web servers and web applications, so one must use a safer browser during important transactions to protect ourself falling into such crimes

B) Cloud Computing Services

Today every company either small, medium or large size companies are slowly adopting cloud service. It shows that world is moving towards cloud technology. This latest trend presents a huge challenge for cyber security, as traffic can go around traditional points of inspection. Also, 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. Cloud services are developing their own models still a lot of issues are being brought up about their security, cloud may provide immense opportunity but with this evolving technology its security concerns are also getting increased.

C) Mobile Networks

We can connect to anyone in any part of world through mobile networks, but for these mobile network's security is a very big concern. 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. Further mobile networks are highly prone to these cybercrimes a lot of care must be taken in case of their security issues. We must always think about the security issues of these mobile networks.

D) IPv6 Protocol

IPv6 is the new Internet protocol which is replacing IPv4, which has been a backbone of our networks in general and the Internet at large. Protection of 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. So, it is better to switch to IPv6 as soon as possible to reduce the risk regarding cybercrimes.

E) Encryption of the code

Encryption is the process of encoding messages in such a way that 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.

The above are some of trends changing the face of cyber security in this world. The top threats for networks and cyber security are remote procedure call, SQL Injection, Browser and Cross-site scripting

V. CYBER SECURITY IN SOCIAL MEDIA

As world is getting connected on social media on a large scale, social media companies should find new ways to protect customer's personal information as Social media plays huge role in cyber security and will contribute a lot personal cyber threats. Since social media or social networking sites are almost used by most of them every day it has become a huge platform for the cyber criminals for hacking private information and stealing valuable data.

In a world where we're quick to give up our personal information, companies have to ensure they're just as quick in identifying threats, responding in real time, and avoiding a breach of any kind. Since people are easily attracted by these social media the hackers use them as a bait to get the information and the data they require. 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.

Though social media can be used for cybercrimes 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 also one must handle social media by using certain policies and right technologies.

VI. TECHNIQUES FOR CYBER SECURITY

A) Password security and access control:

The username and passwords are been a fundamental way of protecting an individual's information. This is a main and first measure taken to protect personal information from attacker

B) Data Authentication

The documents that we download or we receive must be authenticated before opening it and check the origination point is trustable or not. Authenticating of these documents is usually done by the anti-virus software present in the devices so its essential to have a good anti-virus installed in your device.

C) Malware Scanners

Malware Scanners 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

D) 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.

E) Anti-Virus

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.

VII. Ethics to prevent cyber attacks

Cyber ethics are nothing but the code of the internet. Practicing these, there are good chances of us using the internet in a proper and safer way.

- *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*
- *Use internet legally, 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.*
- *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 a trouble.*
- *Always adhere to copyrighted information and download games or videos only if they are permissible.*
- *When you're online never pretend to the other person, and never try to create fake accounts on someone else.*
- *Never try to send any kind of malware to other's systems and make them corrupt.*

These are few cyber ethics that one must follow while using the internet.

VIII. Conclusion

Cyber security is vast topic that is very important because world id becoming highly dependable on internet and getting interconnect at very high speed. Internet is used to carry out critical truncations and it is becoming essential to protect these transactions from any kind of attacks. The latest and disruptive 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 perfect solution for cybercrimes but we should try our level best to minimize them in order to have a safe and secure future in cyber space.

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 " by G.Nikhita Reddy, G.J.Ugander Reddy

[6] IEEE Security and Privacy Magazine – IEEECS "Safety Critical Systems – Next Generation "July/ Aug 2013.

[7] Article by BusinessToday.In dated – 23rd Mar 2021 By: Niti Kiran. Link: https://www.businesstoday.in/latest/economy-politics/story/beware-cyber-security-attacks-in-india-grew-194-in-2020-291535-2021-03-23

[8] Article by RepublicWorld.com dated – 23rd Mar 2021. Link: https://www.republicworld.com/technology-news/other-tech-news/dominos-india-faces-cyber-attack-data-of-18-cr-orders-including-personal-info-leaked.html