VIVA-TECH IJRI
ANNUAL RESEARCH JOURNAL
VIVA-TECH INTERNATIONAL JOURNAL FOR RESEARCH AND INNOVATION
ANNUAL RESEARCH JOURNAL
ISSN(ONLINE): 2581-7280

Cyber Security: Issues, Challenges and Risks

Vinay Chhapre[1], Prof. Krutika Vartak[2]
[1](Department of MCA, Viva School Of MCA/ University of Mumbai, India)
[2](Department of MCA, Viva School Of MCA/ University of Mumbai, India)

Abstract :*Cyber Security is a crucial and rising part of concern in the present age with a rapid increase in the graph of digitization. And with an increase in the activities in cyberspace, there is also an increase in the cyber-crimes. Handling the huge volumes of data with security has become an inevitable need of the hour. Antivirus software, Firewalls, and other technological solutions help to secure this data but are not sufficient enough to prevent the cybercrooks from destructing the network and stealing confidential information. This paper mainly focuses on the issues and challenges faced by cybersecurity. It also discusses the risks, cybersecurity techniques to curb cyber-crime, cyber ethics, and cyber trends.*

Keywords -*Challenges, Cyber Ethics, Cyber Security, Cyberspace Dynamics, Systemic Risks*

I. INTRODUCTION

Today a man is able to send and receive any type of information may be an e-mail or an audio or video just with a tap of a button but did we ever imagine how securely his information is being transferred or sent to the destination safely without leaking of his information?? The solution is cybersecurity.

Internet is a rapidly expanding infrastructure in daily life.[1] In today's technical world many latest emerging technologies are changing the future of mankind. But due to these technologies' mankind is finding it difficult to save himself from the cybercrime escalating day by day. Today maximum transactions are done online, so this subject needs special high-quality attention or security for safest transactions. Therefore, this subject is been a latest issue today. The reach of Cybersecurity is not limited to just keeping our data safe but also to other fields like cyberspace etc. Even the latest technologies like E – commerce, cloud computing, net banking etc. also needs to be secured highly.

As these technologies include important data of a person their security is highly recommended. Enhancing Cybersecurity and safeguarding confidential information infrastructures are essential to each nation's safety of economic health. Making the Internet and the users of internet safe have become the important part of development of emerging services and also government policies. So, the technical measures alone cannot save us from any crime, its necessary that there should be a law for preventing and investing all this. Given that today many countries and governments are announcing strict rules on cybersecurity in order to safeguard the important data of its own. Every person on this planet should also educate about Cybersecurity and protect themselves from the Criminal activities.

II. CYBER SPACE DYNAMICS

Cyberspace is interconnectivity of all the digital devices across the globe. When we talk about a technology that connects everyone at a global level, we can only imagine the risks that come along with the unending scope of growth and digital transformations. However, many businesses and governments have released its potential in the digital growth and heavily invests in it. Although, more technical knowledge is required to abate the risks and secure all the transactions taking place in the cyberspace.

This paper will focus on the four major transformative technologies that contributes to the change in the cyberspace dynamics.[2]

2.1 Ubiquitous Connectivity

Distributed computing allows various devices to share the infrastructure while operating as an independent system. However, this system needs hyperconnectivity, availability of the services, sophisticated networks which demands to focus on various factors such as speed, reliability, low latency, agility and other significant factors. Our system has changed increasingly due to these requirements.[2]

2.2 Artificial Intelligence / Advanced Machine Learning

Automating the complex calculations and executing large volumes of data at a higher execution rate has become possible in the cyberspace.[2] The most important factor is that the machines can be trained using the datasets and most of the manual work is automated, even the learning. This ability to process an aggregation of such large data will lead to huge increases in the predictive powers of algorithms.

2.3 Quantum computing

Quantum computers are the future of the world with the capacity to solve a range of huge computations and modelling problems in the nick of a second. These computers will take over the classical computing in a few years. However, higher technological advancements present new risks to the conventional security measures.

2.4 Emerging next-gen approaches

Emerging next-generation approaches to identity and access management will enable new services, applications and operating models, with efficiency and low friction that can support the fast speed and large scale of the emerging cyberspace. [2]

III. CYBER SECURITY CHALLENGES

Privacy and Security will always remain the topmost concerning factors in the cyberspace. Many organizations take all possible measures to provide security to their and their customers' data. In a world where each user's information is present in the social networking sites, commercial sites and other sites, the security is a must to make the users feel safe and secured in the environment. The cyber criminals have access to a huge pool of resources to destroy the sensitive information or misuse the available information to their benefits. Some of the major challenges of the cyberspace, but not limited to, are listed below:

3.1 Advanced Persistent Threats

The advanced persistent threats are the stealth attacks that penetrate the system and goes undetected for a long period of time.[3] The APT malware is designed for specific targeted attack and is not just a typical malware. Many organizations fail to protect themselves from APTs as they capture the highly sensitive information and go unnoticed for a longer period of time. More study and learning are required to fight against the APT.

Below is the lifecycle of advanced persistent threat.

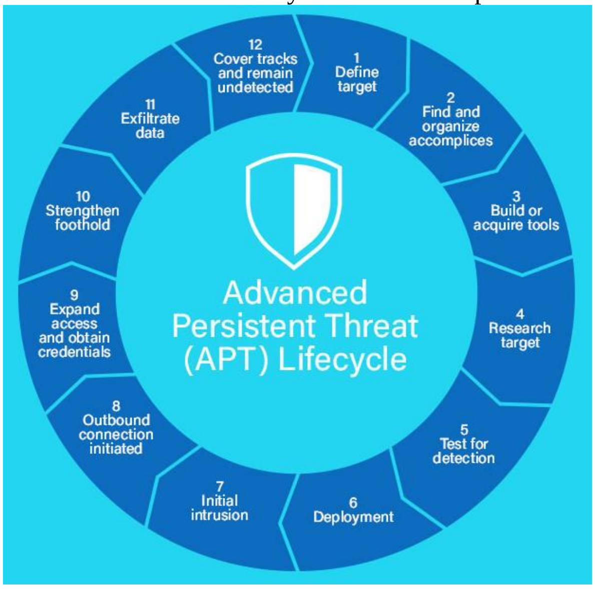
Advanced Persistent Threat (APT) Lifecycle
1 Define target
2 Find and organize accomplices
3 Build or acquire tools
4 Research target
5 Test for detection
6 Deployment
7 Initial intrusion
8 Outbound connection initiated
9 Expand access and obtain credentials
10 Strengthen foothold
11 Exfiltrate data
12 Cover tracks and remain undetected

Figure 1: APT Lifecycle

3.2 Evolution of Ransomware

The Ransomware attacks have increased on a large scale in the past few years. One of the most recent and known is the Petya attack that shut the servers all across the globe and many organizations faced huge losses from it. Ransomwares are one of the types of the APT that penetrates inside the system and encrypts the files.

Once the system gets locked, it demands a ransom to decrypt their data. These malwares usually user bitcoin to demand the ransom as it is difficult to track it.

3.3 IoT Threats

The IoT is an interrelated computing system that transmits data over the network without human intervention.

Each device connected in the internet has a unique identity which makes is possible to differentiate each of the devices. IoT makes it possible to operate the lights, music system, electronic devices, personal assistants, etc. on the touch of a single phone. This is possible due to the connectivity of the devices and its identification through the unique code. But this also means providing a complete access of these systems to the hackers as access to phone will be enough for them to penetrate into your system.

3.4 Cloud Security

Cloud security is an extreme necessity as most of the organizations put their data on the cloud to share the resources, information and services. And even though clouds provide private, public and hybrid networks, the data can still be hacked and the confidentiality can be lost resulting in the huge losses for the organizations.

Many of the organizations prefer to own and manage the Data Center due to this major risk. They need a complete control over their data. However, they pose other risks like natural disasters, insecure API's etc. and to facilitate the smooth flow of daily work, clouds are where the organizations invest.

3.5 Attacks designed with the help of AI and Machine Learning

AI is a boon as well as the bane to the technological advancements as it can make the complex computations easy but also be used to pose a threat by the cyber criminals. As the machine starts learning on its own, it can predict as well as compute the output at a very close precision which can be misused as well. One of the common threats of AI is the Face recognition and morphing. AI bring innovation in the technology as well as threats.

IV. ISSUES AND TRENDS CHANGING CYBER SECURITY

4.1 Web servers

The risks of attacks on web apps to distribute malicious code or to extract data continues. Cyber criminals distribute their malicious code via trusted web servers they've hacked. But information-stealing attacks, many of which get caught by the media, also are a huge threat. Web servers are specially the simplest platform for these criminals to steal the data. Hence, one should use a safe browser specially during important transactions, so they not fall for these cyber-attacks.

4.2 Cloud computing and its services

These days all types of companies small or big, are slowly trying to adapt to cloud services. In short, the world is slowly adopting towards the clouds.[4] This trend presents an immeasurable challenge for cybersecurity. Thus, the number of apps available within the cloud grows, policy control for web application and cloud services also will get to evolve so that to stop the loss of valuable data.

4.3 Mobile Networks

In today's time, we are able to connect to any part of the globe to anyone. But for these networks, security is a huge concern. Nowadays firewalls or other security measures are becoming absorbent as people are using devices such as Desktops, laptops, phones etc. all of these which again require additional securities apart from those existing in the apps used. We should always think about the security risks of these wireless networks. Thus, mobile networks are highly likely to these cyber-crimes. A lot of safety measures must be taken in case of their security issues.[5]

4.4 Encryption of the code

Encryption is the method of encoding mails or any data in such a way that spies or hackers cannot look through it. In an encryption system, the message or data is encrypted using an algorithm, creating it in an unreadable cipher text. This is generally done with the usage of an encryption key, which lay down how the message is to be programmed. Encryption at a very foundation level shields data privacy and its veracity. But higher the use of encryption brings higher challenges in cyber security. Encryption is also used to protect data in its journey, for instance information being transferred by means of networks, for e.g., the Internet, mobile telephones, ecommerce, wireless intercoms, wireless microphones, etc. So, by encrypting the code we can know if there is any outflow of information. Hence the above data are some of the trends altering the aspect of cyber security in the globe.

4.5 APT's and targeted attacks

Advanced Persistent Threat (APT) is a totally a new level of cyber-crime. For long years network security abilities such as web filtering or IPS have played a key part in identifying such targeted attacks, mostly after the early compromise. As hackers grow bolder and engage more vague techniques, network security should integrate with different security services in order to detect these attacks. Hence everyone must improve their security techniques in order to prevent more threats in the future.

V. SYSTEMIC RISKS

Cyber risk not only affects individual financial institutions but has an important systemic dimension. The World Economic Forum (WEF) defines systemic cyber risk as "the risk that a cyber event (attack(s) or other adverse event(s)) at an individual component of a critical infrastructure ecosystem will cause significant delay, denial, breakdown, disruption or loss, such that services are impacted not only in the originating component but consequences also cascade into related (logically and/or geographically) ecosystem components, resulting in significant adverse effects to public health or safety, economic security or national security." [3]

5.1 Scale and Criticality

With an increase in the connectivity of new devices in the internet, there is an increased risk of the attacks as the number of available resources is soaring. The CIA triad – Confidentiality, Integrity and Availability is becoming difficult to maintain as more and more devices are connecting to the internet. The potential implications in terms of compromise for industry and society are becoming more severe.

5.2 Interdependency

The complexity of the interconnections is rising as we witness more and more type of devices entering the global interconnection. Nowadays, we have digital watches, health care devices, personal assistants, mobile phones, etc. This also means cascading effect of the attacks. Attack on one ecosystem can prove dangerous to the other information as well. Appropriate levels of protection are needed to secure these gaps and assign accountability to the end-to-end processes.

5.3 Shared Resources

The probability of the damage for the attack increases when the resources share some kind of infrastructure, services or other resources. As the pool of the resources increase, the surface area for the attacks increases too. There is a risk of collateral damage occurring as a result of targeted attacks against a single client via this shared infrastructure. Identifying the critical shared resources, who owns them and their key dependencies is a complex task.[6]

VI. CYBER SECURITY TECHNIQUES

6.1 Access control and password security

The idea of user name and password has been primal way of protecting our data. This might be one of the first measures about cyber security. [7][8]

6.2 Authentication of data

The documents that we collect should always be authenticated before downloading that is it must be checked if it has derived from a trusted and a steadfast source and that they are not reformed. Authenticating of these data is usually done by the anti-virus software program present in the devices. Hence a good anti-virus software is also crucial to protect the devices from virus attacks.

6.3 Malware scanners

This software that usually scans all the files and docs present in the system for malicious code or destructive viruses. Worms, Viruses, and Trojan horses are examples of malicious software that are often assembled together and denoted to as malware.

6.4 Firewalls

A firewall is a software that helps detect worms, viruses and hackers that try to maliciously harm your computer over the Internet. All messages incoming or outgoing the internet permit through the firewall present, which scrutinizes each message and obstructs those that do not meet the specific criteria of the security. Hence firewalls play a significant role in detecting the malware. [7][8]

6.5 Anti-virus software

Antivirus software is a software program that detects and prevents later takes action to deactivate or eliminate malicious software programs, such as worms and viruses. Maximum anti-viruses have a feature to update itself automatically so that whenever a new virus or a malware is found it can take respective action according to the update. An anti-virus software is a must and basic requirement for every system.

VII. CYBER ETHICS

Cyber Ethics are nothing but the code or rules of Internet which if we follow while browsing or surfing the internet, we can be much more proper and safer. Some of the ethics are listed down below:

- Do use the Internet to interact and communicate with friends and family. Instant messaging and email make it easy to share different ideas and informationwith any people across halfway around the world, stay in touch with friends and family members and also to communicate with work colleagues.
- Don’t try to bully on the Internet. Do not share any pictures of people and call names, or do anything which can hurt anyone.
- Internet is known as the world’s largest library with any type of data or information on any subject area of any topic, so that’s why using the internet in a legal and correct way is always essential.
- Do not ever try to operate any other account without the owner’s permission using their passwords.
- Never try to corrupt systems by sending any type of viruses or malware, its illegal.
- Never share any type of your personal data or information to anyone as there is a high chance of them misusing it and at the end of it you would be in trouble.
- We must never pretend to be someone else by creating fake accounts and fake ids as it would call a great trouble to you and that other person.
- Always be careful of copyrighted information such as downloadable games and videos and download it only they are permitted to.

These are some of the cyber ethics everyone must follow while browsing the internet. We are always taught proper rules from very early stages of life and the same we apply here in cyber space.

VIII. CONCLUSION

Cyber-security is becoming more significant in light of the fact that the world is becoming extremely inter-connected with networks being used to accomplish critical transactions. Cyber-crime continues to increase each year at a tremendous rate because, with more critical information being effectively accessible in cyberspace, more territory for the threat attacks is exposed to the attacker. Yet the positive aspect is thatsecurity has become conspicuous and of the highest priority for the senior leadership teams and organizations are tightening their approach towards strengthening cybersecurity.

To date, there is no solution which we can exclaim as immaculate, however as a responsible user, one can always make sure to follow the cyber ethics for their data security and report any pernicious activity if found. It also brings a great responsibility on the national and internationaladministration to actualize strict laws against cyber-crimes and invest in projects that pursuereinforcing security and rather than viewing the speculation as a monetary burden, convert this need into a business empowering influence.

REFERENCES

[1] Hena Iqbal, Ghassan Al-Utaibi, Om Prakash Bohra,“The Reality of Technologies for Cyber SecurityChallenges”, *International Journal of Recent Technology and Engineering (IJRTE), Volume-9 Issue-1,* May 2020, pp. 2277-3878.

[2] World Economic Forum (WEF), In collaboration with the University of Oxford, “Cybersecurity, emerging technology and systemic risk”, *Insight Report, November 2020.*

[3] World Economic Forum (WEF), “Understanding Systemic Cyber Risk,” *Global Agenda Council on Risk & Resilience, White Paper, October 2016*.

[4] G.Nikhita Reddy, G.J.Ugander Reddy (2013), *“ Study of Cloud Computing in healthcare Industry”, International Journal of Scientific & Engineering Research, Volume 4, Issue 9*, September-2013.

[5] Nina Godbole and SunitBelapure,*Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives (*New Delhi, Wiley India Pvt Ltd., 2011).

[6] Edward G. Amoroso,in Computer and Information Security Handbook (Third Edition), *Software-Defined Networking and Network Function Virtualization Security*(2017).

[7] Mr. Suresh Patle, Mr. MurlidharKatre*, "A study of Cyber Security Challenges and its EmergningTrends on Latest Technologies", International Education Scientific Research Journal, Volume-6, Issue-10,*October 2020, pp.2455-295X.

[8] G. Nikitha Reddy, G.J. Ugander Reddy*, "A study of Cyber Security Challenges and its EmergningTrends on Latest Technologies"*, 2014.

[9] R. Bloomfield and J. Lala, *"Safety-Critical Systems: The Next Generation", IEEE Security & Privacy, Vol. 11, No. 4,* pp. 11-13, July-Aug 2013.

[10] James Lyne, *Eight Trends Changing Network Security*, a Sophos Article 04. 12v1.dNA

[11] Peter Sommer, Ian Brown, *Reducing Systemic CyberSecurity Risk*, OECD/IFP ProjectonFuture Global Shocks, 2011

[12] Backhouse, J. and G. Dhillon, *"Information system security management in the new millennium", Communications of the ACM, Vol. 43, No. 7*, pp. 125-128, 2000.

[13] Michael S. Fischer, *Top 10 Cybersecurity Trends for Financial Services in 2015*, Article in2014.

[14] Booz Allen Hamilton, *Top Ten Cybersecurity Trends for Financial Services in 2012*, Article in2012.

[15] FinTech Futures, *Cyber landscape, threats and trends in financial services*,Article in2019.