IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, November 2022
Impact Factor: 6.252

A Study of Cybersecurity and its Role in Information Technology along with the Emerging Trends and Latest Technologies

G. Prem Prathyush[1] and G. Pavan Durga Kumar[2]
B.Tech. Students, Department of Information Technology[1,2]
Prasad V. Potluri Siddhartha Institute of Technology, Vijayawada, Andhra Pradesh, India

Abstract: *Cybersecurity place and significant role in the field of information technology. Providing security for information has become one of the biggest challenges in the present day. The first thing that comes to our mind when we think of cybersecurity is the amounts of cybercrimes which are increasing day by day. Various governments and companies are taking many measures to prevent these cybercrimes. Despite these various measures cybersecurity is still an excessively big concern to many individuals. This paper focuses on challenges faced by cyber security during the development of the latest technologies. It also focuses on various cybersecurity techniques, ethics and the trends changing the face of cyber security.*

Keywords: Cyber Security, Cybercrime, Cyber Ethics, Social Media, Cloud Computing.

I. INTRODUCTION

In the present modern world, a person is able to send and receive any kind of information or data maybe an e-mail or a video or audio just by the click of a button at the tip of his fingers, but do we think how secure his or her data is being transmitted or sent to the other person without any leakage of information? The answer lies in cybersecurity. in the modern times Internet is the fastest growing infrastructure in everyday life many latest technologies are changing the face of the humankind. With the rise in these emerging technologies, we are not able to safeguard our confidential information in a fight effective manner and as a result streams are showing us their every day by day. A recent research survey conducted shows that today more than 60% of the total commercial transactions are online so this build requires equality of unity transparent and best transactions. As a result, cybersecurity has become a latest issue. The scope of cyber security is so vast that it is not limited to just securing information in the IT industry but also to various he is like cyberspace and cloud.

Several modern-day technologies like cloud computing, mobile computing, ecommerce net banking etc also require an elevated level of security. Since these technologies hold up prominent information regarding a person their security has become a key thing. Improving cyber security and safeguarding critical information including infrastructures are important to each nation security and economic development stop making the Internet safer has been an integral part for the development of new services as well as government policies. The modern war against cybercrime needs a comprehensive and safer approach for the technical measures alone cannot prevent any crime it is important that the law enforcement agencies are allowed to investigate and prosecute cybercrime effectively today nations and governments are improved laws on security in order to enter the leakage of information which is important every individual participated on basic knowledge of to save themselves from these increasing cybercrimes and gain some knowledge on cybersecurity.

II. CYBERCRIME

Cybercrime refers to the criminal conduct committed with the aid of computer, or any electronic devices connected to the Internet. Individuals or small group of people with little technology technical knowledge and highly organized worldwide criminal groups with relatively talented developers and specialists can engage in cybercrime to make money cyber criminals engage in a wide range of profit driven criminal acts including stealing and reselling identities and

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, November 2022
Impact Factor: 6.252

fraudulently utilizing credit cards to obtain funds. The expanding list of cybercrimes includes crimes that have been made possible by computers
such as network intrusions and the dissemination of computer viruses 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 add nations. In normal terms cybercrime can be defined as a crime which is committed with the help of a computer connected to the Internet. With every day passing technology is playing a significant role in a person's life the cybercrimes also will increase along with the technological advancements.
Studies clearly show that most companies are not only vulnerable to cyber security issues, but they are also easy targets. As a result, it is imperative that companies make cybersecurity awareness prevention and security best practices apart of their culture by doing this companies will at least stand a chance of fighting against data loss something that majority of companies around the world. At a growth rate of 15% year over year cybersecurity ventures also report that cybercrime represents the greatest transfer of economic wealth in history.

III. CYBERSECURITY

We are currently living in a world play all the information is maintained in either digital or cyber form. Cyber security is the application of technologies processes and controls to protect systems networks programs devices and data from cyber-attacks its goal is to reduce the risk of cyber-attacks and protect against unauthorized exploitation of systems networks and technologies privacy and security of data will always be top security measures that any organization takes care. It is a mistake to believe that you are of no interest to cyber attackers.

Every individual who is connected to the Internet needs cybersecurity because most cyber-attacks are automated and aim to exploit common vulnerabilities rather than specific websites or organizations. Cybersecurity is crucial because it safeguards all types of data against theft and loss. Sensitive data protected health information (PHI), personally identifiable information (PII), intellectual property, personal information, data, and government and business information systems are all included.
Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, November 2022
Impact Factor: 6.252

- **Network security** is that the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.
- **Application security** focuses on keeping software and devices freed from threats. A compromised application could provide access to the info it's designed to protect. Successful security begins in the design stage, well before a program or device is deployed.
- **Information security** protects the integrity and privacy of knowledge, both in storage and in transit.
- **Operational security** includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and therefore the procedures that determine how and where data could also be stored or shared all fall under this umbrella.
- **Disaster recovery and business continuity** define how a corporation responds to a cybersecurity incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and knowledge to return to the same operating capacity as before the event. Business continuity is that the plan the organization falls back on while trying to work without certain resources.
- **End-user education** addresses the foremost unpredictable cyber-security factor: people. Anyone can accidentally introduce an epidemic to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not connect unidentified USB drives, and various other important lessons is significant for the security of any organization.

IV. TRENDS CHANGING CYBERSECURITY

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

4.1 Web Servers

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 eye of media, also are 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 info. Hence one should use a safer browser, especially during important transactions so as not to fall prey to these crimes.

4.2 Cloud Computing and its Services

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

4.3 APT's and Targeted Attacks APT

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

4.4 Mobile Networks

Today we will connect to anyone in any part of the world. except for these mobile network's security is a very big concern. nowadays firewalls and other security measures are becoming porous as people are using devices like tablets, phones, PC's etc all of which again require extra securities apart from those present in the applications used. We should

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, November 2022
Impact Factor: 6.252

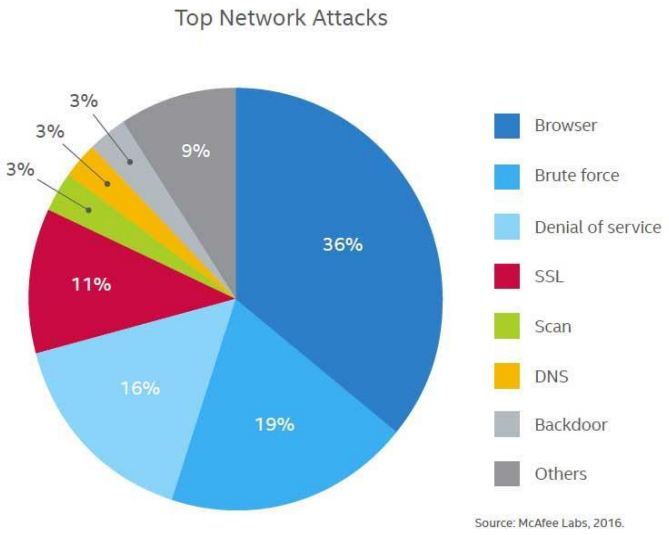
think about the security issues of these mobile networks. Further mobile networks are highly susceptible to these cybercrimes and a lot of care must be taken just in case of their security issues.

4.5 IPv6

New internet protocol IPv6 is that the new Internet protocol which is replacing IPv4 (the older version), which has been a backbone of our networks generally and the web at large. Protecting IPv6 is not just an issue of porting IPv4 capabilities. While IPv6 may be a wholesale replacement in making more IP addresses available, there are some very fundamental changes to the protocol which require to be considered in security policy. Hence, it's always better to switch to IPv6 as soon as possible in order to scale back the risks regarding cybercrime.

4.6 Encryption of the Code

Encryption is that 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 often usually done with the use of an encryption key, which specifies how the message is to be encoded. Encryption at a really beginning level protects data privacy and its integrity. But more use of encryption brings more challenges in cyber security. Encryption is additionally used to protect data in transit, for instance data being transferred via networks (e.g., the Internet, ecommerce), mobile telephones, wireless microphones, wireless intercoms etc. Hence by encrypting the code one can know if there's any leakage of information.



V. CYBERSECURITY TECHNIQUES

5.1 Access Control and Password Security

It is important to control who has access to our information for this the fundamental way of protecting is the concept of username and password. This is one of the first measures of cybersecurity

5.2 Authentication of Data

Before downloading it is especially important that the documents which are received must be always authenticated and checked to see if it has originated from a reliable source without being altered. The authentication is performed by antivirus software, so it is essential just to have antivirus for protection from viruses.

5.3 Malware Scanners

The grouping of virus worms, and Trojan horses are referred to as malware. Malware scanners usually scan all the files and documents for malicious code or viruses.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, November 2022
Impact Factor: 6.252

5.4 Firewalls

Firewall is a system designed to prevent unauthorized access. You can implement a security system in either hardware or software form are a combination of both. firewalls prevent unauthorized Internet users from accessing private networks connected to the Internet.

5.5 Antivirus Software

Antivirus software is a program which makes you safe from potentially malicious and unwanted programs from being executed in your device while you are over the Internet or offline. Most antivirus programs include an auto update feature that enables the program to download profiles of new viruses so that it can check for them as soon as they are discovered. It is basic for every system.

VI. CYBER ETHICS

The code of the Internet is known as cyberethic. It is important that we practice these cyberethics as it teaches us to use the Internet in a proper and safer way. They are

Use the Internet to communicate an interact with people who are far away from you.it is easy to stay in touch with people who are around the world

Do not be a bully on the Internet do not perform name calling or hurt them

Internet is the world's biggest library so using it that matter is very much important

Never share your personal information online to anyone

Never pretend to be a fake person on the Internet or use fake accounts

These are a few cyber ethics one must follow while using the Internet. With proper ethics the Internet can be a safe place for everyone.

VII. CONCLUSION

Cybersecurity is one of the vast topics and quickly developing fields in the world as every device is being connected to the Internet. Cybercrime continues to show an upward trend every year. Each day new cyber threats are challenging organizations which are not only about securing infrastructure but also on how to require new platforms and intelligence to counter cybercrimes. There is no perfect solution to cybercrimes, but we must 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- SunitBelapure 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]. IEEE Security and Privacy Magazine – IEEECS "Safety Critical Systems – Next Generation "July/ Aug 2013.
[6]. CIO Asia, September 3rd , H1 2013: Cyber security in malasia by Avanthi Kumar
[7]. 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
[8]. https://www.kaspersky.co.in/resource-center/definitions/what-is-cyber-security