WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Glossary of the Difficulties in Cyber Security and its Emerging Trend in the Latest Technology

Dr. Mohd Zuber[1], *Dr. Sheema Quereshi*[2]

[1]**Associate professor, Madhyanchal Professional University, Bhopal, India**
[2]**Assistant Professor, Govt. College Aron., India**

DOI: https://doi.org/10.55248/gengpi.4.1023.102636

ABSTRACT

Cyber security is essential to the information technology industry. One of the biggest problems in today's world is information security. The first thing that springs to mind when we consider cyber security is "cyber crimes," which are getting worse every day. Numerous governments and businesses are implementing numerous strategies to combat these cybercrimes. Cyber security, in addition to its numerous measures, continues to cause great anxiety in many. The primary topic of this paper is the difficulties that modern technology presents for cyber security. It also emphasizes the most recent developments in cyber security methods, morality, and fashions that are redefining the field.

Keywords: cyber security, cyber crime, cyber ethics, social media, cloud computing, android apps.

1. INTRODUCTION

With the push of a button, man may send and receive any type of data these days, including audio and video files, emails, and videos. However, has he ever considered how securely his data is transported or sent to other people, ensuring that no information is lost? The Internet is currently the fastest-growing form of communication in daily life. The state of technology today is transforming humanity through the use of numerous cutting-edge technologies. However, as a result of this ever-evolving technology, we are unable to protect our personal information as effectively, which is why cybercrimes are increasing daily in the modern era. Since over 60% of all profitable transactions are now completed online, this industry requires a high level of security to ensure the most transparent and successful transactions. Cyber security has so emerged as a contemporary concern. Cyber security covers a wide range of areas, including cyberspace and other domains, in addition to protecting data in the IT business.

Even the most recent technology, such as online banking, cloud computing, mobile computing, and e-commerce, demands a high level of security. These technologies' security has become essential since they include some very important personal data. For the security and economic well-being of every country, it is imperative to strengthen cyber security and safeguard vulnerable information infrastructures. Increasing Internet safety has become crucial for the creation of innovative services in addition to governmental planning. A thorough and safer methodology is needed to combat cybercrime. It is dangerous that law enforcement organizations are allowed to look into and successfully prosecute cybercrimes. Strict rules on cyber security are being imposed by many governments and countries these days in an effort to prevent the loss of some crucial data. Each person needs to be knowledgeable about cyber security in order to protect themselves from the increasing number of cybercrimes.

2. CYBER CRIME

Any illegal activity that primarily charges and steals from computers is referred to as cyber crime. The definition of cybercrime as defined by the U.S. Department of Justice now includes any unlawful behavior that stores proof on a computer. Cybercrimes are becoming more and more common. These include crimes that are made possible by computers, like network intrusions and the spread of computer viruses, as well as computer-based versions of crimes that are still possible, like identity theft, stalking, bullying, and terrorism, which are becoming major issues for individuals and countries. Often, in everyday language, cybercrime can be distinguished as crimes carried out via a computer and the internet to steal someone's identity, sell illicit goods, harass victims, or interfere with activities in a malevolent way. The increasing role that technology plays in people's lives means that, as technology develops, so too will the number of cyber crimes.

3. CYBER SECURITY

Data security and privacy will always be an organization's top priorities when it comes to safety. In the world in which we currently live, all information is kept in digital or cyber form. Users of social networking sites can collaborate with friends and family in a safe environment. Cybercriminals will continue to target social media sites in the case of home users in order to steal personal information. A person needs to take all necessary security precautions not just when using social networking sites but also when conducting bank transactions.

Incidents	Jan- June 2012	Jan- June 2013	% Increase/ (decrease)
Fraud	2439	2480	2
Intrusion	2203	1726	(22)
Spam	291	614	111
Malicious code	353	452	25
Cyber Harassment	173	233	35
Content related	10	42	320
Intrusion Attempts	55	34	(56)
Denial of services	12	10	(17)
Vulnerability reports	45	12	(76)
Total	581	5592	

Table I

New assaults on Android-powered smart phones are coming, but they won't be very widespread. Because tablets use the same operating system as smart phones, the same virus that targets those platforms will eventually target them. Though far fewer than for PCs, the quantity of malware specimens for Macs would continue to rise. These are some of the anticipated trends in cyber security. Since Windows 8 will enable users to create apps for almost any device (PCs, tablets, and smart phones running Windows 8), it will likely be possible to create malicious apps similar to those for Android.

4. TRENDS CHANGING CYBER SECURITY

Cyber security dangers are evident in the above review of Cyber security Incidents reported to Cyber999 in Malaysia between January and June of 2012 and 2013. Security measures are increasing in tandem with the rise in crime. As per the analysis of U.S. Silicon Valley Bank conducted a survey of technology and healthcare leaders across the country and discovered that businesses consider cyber attacks to be a serious risk to their data and overall viability.

The majority of businesses are preparing for when, not if, cyber attacks occur. Only one-third of businesses are completely confident in the security of their information, and even fewer are confident in the security measures of their business associates. 98% of businesses are maintaining or growing their cyber security assets, and of those, half are increasing assets dedicated to online attacks this year.

Some of the trends that are significantly affecting cyber security are listed below.

Web servers:

Attacks against web apps with the intention of obtaining data or spreading harmful code are still a possibility. Cybercriminals use hacked legitimate web servers to distribute their malicious programs. However, there is also a serious risk from data-stealing hacks, many of which are publicized by the media. We now need to give defensive web servers and online applications more attention. The most effective platform for these cybercriminals to steal data is web servers. Therefore, in order to avoid becoming a victim of these crimes, it is imperative that one always uses a safer browser, especially during crucial transactions.

Cloud computing and its services

These days, cloud services are being progressively adopted by all sizes of businesses, small and large. Stated differently, the earth is gradually approaching the clouds. The ability of traffic to evade traditional points of inspection makes this most recent trend extremely challenging for cyber security. Policy controls for web apps and cloud services will also need to be developed as the number of applications available in the cloud increases in order to stop the loss of important data. Even while cloud services are growing their own business models, many security-related concerns are still being raised. Although there are a lot of potential in the cloud, it's important to remember that as the cloud grows, so do security risks.

Under assault and with APTs

Advanced Persistent Threat, or APT, is a completely new class of cybercrime malware. For many years, network security features like intrusion prevention systems and web filtering have been crucial in detecting intrusions of this kind (usually after the first infection). Network security must collaborate with other security services to detect attacks as attackers become more daring and use more elusive tactics. Therefore, in order to stop new risks from emerging in the future, we must upgrade our security procedures.

Mobile Networks

We can now communicate with anyone, anywhere in the globe. But security is a major worry for these mobile networks. Nowadays, as more people use devices like tablets, phones, PCs, and other gadgets, firewalls and other security measures are becoming more and more important. These devices require additional security measures on top of those offered by the programs they use. We need to be aware of these mobile networks' security concerns at all times. Furthermore, mobile networks are particularly vulnerable to these cybercrimes, thus caution must be exercised when it comes to any security concerns.

The new internet protocol, IPv6

The earlier IPv4 system, which served as the backbone of both the Internet and our networks generally, has been replaced by the new IPv6, or Internet system. It takes more than merely migrating IPv4 capabilities to secure IPv6. Although IPv6 is a complete replacement for IPv4 in terms of increasing the number of IP addresses available, there are certain fundamental protocol changes that must be evaluated in terms of security policy. Therefore, in order to reduce the dangers associated with cybercrime, it is always preferable to make the changeover to IPv6 as soon as possible.

The code's encryption

The process of encoding messages (or information) so that hackers or malware droppers cannot read it is known as encryption. An encryption system turns a message or piece of data into unintelligible cipher text by encrypting it with an encryption algorithm. An encryption key, which specifies how the message is to be encoded, is typically used to do this. Data integrity and privacy are safeguarded from the very beginning using encryption. However, increased encryption use also means more cyber security challenges. Additionally, data being exchanged across networks (such as the Internet and e-commerce), mobile phones, wireless microphones, wireless intercoms, etc., are protected by encryption. Hence by encrypting the code one can know if there is any escape of information.

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.

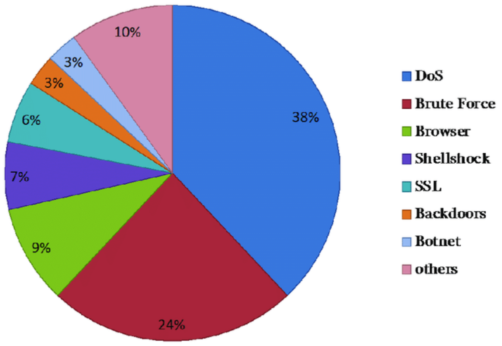

Fig -1

The above pie chart shows about the major threats for networks and cyber security.

5.Social media's accountability for cyber security

Businesses must come up with innovative strategies to protect personal data since we live in a world where connectivity is growing and social interaction is expected. Social networking is very important for cyber security and will make a significant contribution to certain cyber threats. Employee acceptance of social media is rapidly increasing, as is the risk of abuse. Since the majority of people utilize social media or social networking sites on a daily basis, it has grown to be a huge platform for cybercriminals to steal valuable data and hack sensitive information.

In a world where people are quick to divulge personal information, businesses need to ensure that they are equally quick to recognize dangers, act quickly, and prevent any kind of breach. Since social media platforms captivate users, hackers leverage them as a draw to obtain the data and information they need. Therefore, users need to take the necessary precautions, especially when using social media, to ensure that their information is kept safe. The fundamental difficulty that social media poses for corporations is people's ability to disseminate information to millions of viewers. Social media not only gives everyone the ability to spread economically sensitive information, but it also gives them the ability to spread false information, which may be just as detrimental. One of the emerging threats identified in the Global Risks 2013 report is the exponential rise in incorrect information spread via social media.

Even if social media can be exploited for cybercrimes, many businesses rely too heavily on it for publicity, thus they cannot afford to cease utilizing it. Alternatively, they need to have solutions that alert them to the problem so they can address it before any real harm is done. But in order to avoid problems, businesses should understand this, understand how important it is to analyze the data from social discussions above all else, and offer suitable security solutions. The appropriate technologies and well-reasoned policies must be used for managing social media.

5. CYBER SECURITY TECHNIQUES

Controlled access and secure passwords

The idea of a user name and password has been a fundamental method of protecting personal data. This can be among the initial steps taken in terms of cyber security.

Authentication of data

The documents we get must always be authentic; therefore, before downloading, they must be verified to have come from a reputable and trustworthy source and to have not been altered. Typically, the antivirus program included in the plan is responsible for authenticating these papers. Thus, in order to shield the gadgets from viruses, effective antivirus software is also required.

Malware scanners

This software typically checks all of the system's files and papers for malicious viruses or hostile code. Malicious software is generally referred to as malware and includes programs like Trojan horses, worms, and viruses.

Firewalls

A firewall is a hardware device or software application that helps block viruses, worms, and hackers from infecting your computer through the Internet. Every message entering the network or leaving it is filtered by the firewall, which checks each one and deletes any that don't fit certain security requirements. Firewalls are therefore crucial for identifying malware.

Anti-virus software

Computer programs known as antivirus software are designed to identify, stop, and eliminate harmful software, including worms and viruses. Antivirus software typically has an auto-update capability that allows it to download virus profiles as soon as new ones are found, allowing it to scan for them first. For any machine, antivirus software is an absolute must.

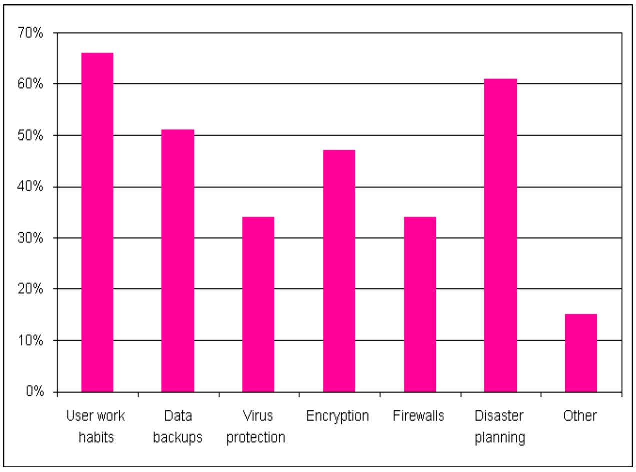

Table II: Techniques on cyber security

6. A cyber-ethic

The internet's code is all that cyber ethics are. We have a fair chance of utilizing the internet responsibly and safely when we follow these cyber principles. Here are a handful of them:

- DO engage in social interaction and communication over the Internet. Email and instant messaging facilitate communication with individuals of all ages at work, with friends and family, and with those across town or on the other side of the globe.
- Avoid appearing menacing on the internet. Never try to hurt someone by calling them names, lying about them, sending offensive images of them, or doing anything else.
- Since the Internet is widely regarded as the world's largest library, containing knowledge on any subject under the sun, it is always imperative to use it responsibly and in accordance with the law.

- Don't use other people's passwords to get access to their accounts.
- It is never advisable to attempt infecting other people's PCs with malware.
- Never divulge your personal information to anyone, as there's a high likelihood of it being misused by others, which could land you in hot water.
- When using the internet, avoid making up stories about other people and refrain from creating false accounts on their behalf, as this could put both of you and them in danger.
- Only upload content that is protected by copyright here, and only download videos or games that are allowed.

A few cyber ethics that one should follow when utilizing the internet are listed above. We have always been taught acceptable norms from an early age, and the same is true in cyberspace.

7. CONCLUSION

With networks being utilized for vital transactions, computer security is a broad topic that is becoming more important as the world gets more uniform. With every New Year that goes by, cybercrime and information security continue to take different turns. In addition to requiring new platforms and ingenuity to secure communications, the newest and disruptive technologies are placing demands on companies about intimidation and new cyber tools that are discovered on a daily basis. While there is no perfect way to stop cybercrimes, we should make every effort to lower their number so that people can continue using the internet safely and securely in the future.

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. CIO Asia, September 3rd, H1 2013: Cyber security in malasia by Avanthi Kumar.