International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 06 | Jun 2022 www.irjet.net p-ISSN: 2395-0072

Cyber Security Challenges on Latest Technologies

Anusha Patil[1], Dr. Samita K[2]

[1]Student Dept. Of MCA, Dayananda Sagar College of Engineering, Bangalore, Karnataka, India
[2]Associate Professor, Dept. Of MCA, Dayananda Sagar College of Engineering, Bangalore, Karnataka, India

---

Abstract -Data innovation relies heavily on information security, which plays a major role. Data security has become possibly the most challenging issue in the modern world. 'Digital wrongdoings,' which are growing exponentially on a daily basis, always come to mind when people think of digital security. There are a variety of measures being taken by governments and organizations around the world to stop these online crime. Network security is still a major concern for many people, despite the implementation of many solutions. It is the focus of this study to examine the most current challenges to digital security. This article also discusses some of the most recent developments in network security, including new ethical standards and emerging patterns.

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

1. INTRODUCTION

Modern technology allows us to instantly transmit and receive virtually any type of data, including audio and video files. But, even if we can send and receive data via email, sound, and video files, all with the press of a button, have we ever considered how securely our data is transported to and from the other party? The response lies in digital protection.

Today, the Internet is the fastest-growing structure in our daily lives. It's becoming increasingly common to see new technological advancements reshaping the world around us. Digital wrongdoings are on the rise every day because of these new technologies, which make it impossible for us to protect our private information in an efficient manner. High levels of security are vital in today's environment, where more than 60% of all commercial transactions are conducted online. Digital security has now become a major concern. More than only data in the IT business is covered by digital protection; it extends into other areas like the internet and so on[4].

Even the most recent technological improvements, such as cloud computing, flexible registration, E-commerce, online banking, and so on, necessitate an increased level of security.

The security of these inventions has become a need due to the fact that they contain sensitive data about an individual. Every country's security and economic growth depend on enhancing digital security and protecting key data foundations. Legislative and administrative growth depends on making the Web more secure (as well as protecting Internet users). There has to be a more comprehensive and secure approach to combating digital misconduct. In order to prevent all misconduct, policing authorities must be able to investigate and punish digital crimes in the real world. Many countries and state-run institutions are imposing strict regulations on digital protections in order to prevent the loss of crucial data. Each and every person must be prepared for this digital security and protect themselves from these increasing digital violations[4].

2.CYBER CRIME

The phrase "digital wrongdoing" refers to any criminal activity in which the use of a PC is a primary means of committing the crime or conducting a burglary. If a crime can be proven using a computer, it is considered digital wrongdoing by the US Division of Equity. It's becoming increasingly common for PCs to be used to perpetrate crimes that were previously unimaginable due to human error, such as disruptions to businesses and the spread of computer viruses. However, PCs can also be used to perpetrate crimes that were previously illegal but have now taken on new dimensions due to the widespread use of PCs. "Digital wrongdoing" describes crimes performed with a computer and the internet to steal somebody's identity, sell stolen property, find victims or disrupt activities with noxious software as "digital wrongdoing." Every time a new technological advancement is made, it brings with it an increase in the importance of digital wrongdoing[2].

2. NETWORK SECURITY

Any association's main priority will always be protecting and securing its membership' personal data. As a result, we're now living in a society where everything is stored electronically. Long-distance informal communication destinations allow consumers to cooperate with loved ones in a secure setting. Digital thieves would then proceed to target web-based entertainment venues in order to steal private information from customers at home. Individuals should accept all needed safety measures in person-to-person conversation as well as during bank exchanges[2].

- 98 percent of firms are maintaining or extending their network security assets, and half of those are doing so in order to better protect against cyber predators in the next year.

- The majority of companies are geared up to deal with cyber attacks when they occur rather than if they do.
- 33% of respondents are confident that their data is safe, but less confident about their colleagues' efforts to keep it that way.

Despite the fact that there will be new approaches to Android-based products, it won't be a huge undertaking. The fact that tablets and PDAs share a similar functioning foundation suggests that the same virus may soon identify them as those phases of the device life cycle. Malware samples for Macs are increasing, although at a far slower rate than those for PCs. Microsoft's new operating system, Windows 8, makes it feasible for users to write programmes that operate on virtually any device running Windows 8 (PCs, tablets, and smart mobile phones). Digital security experts expect a number of developments in the near future.

4. TRENDS CHENGING CYBER SECURITY:

4.1 Web servers

Online applications are still vulnerable to assaults that aim to delete data or spread malicious software. Web servers that have been hacked by digital criminals are used to distribute their malicious code. There is also a risk of information-gathering attacks, the vast majority of which go undetected in the media. Our current focus is on protecting web servers and online applications, and we want it to be even more prominent. These digital lawbreakers make excellent use of web servers as a launching pad for their information heists. In order to avoid becoming a victim of these scams, it is necessary to use a more secure application at all times, especially during large transactions.

4.2 Cloud registering and its administrations

Cloud-based services are progressively being used by all types of businesses, from small to big. As a whole, the globe is getting closer and closer to the mist. Traffic may easily bypass conventional points of evaluation in this most current pattern, making network security a big challenge. To prevent the loss of crucial data, web application strategy controls and cloud service controls must evolve as the number of cloud-based services grows. Security concerns remain despite the fact that cloud administrations are developing their own models. However, it is important to keep in mind that as the cloud expands, so does its security risk.

4.3 API's and designated assaults

API (Advanced Persistent Threat) is a completely new type of digital criminality. Security measures like web filters and intrusion prevention systems (IPS) have long relied on their capacity to distinguish between predictable and unpredictable assaults (generally later the underlying split the difference). Network security should interact with other security administrations to spot attacks as they become bolder and use more questionable tactics. The only way to keep up with current dangers is to keep improving our security measures in the future.

4.4 Mobile Networks

We can now connect with anyone in the globe with current technologies. Whatever the case may be, security is a huge issue for these portable businesses. These days, people are using a variety of gadgets including tablet computers, mobile phones, and computers that require additional security measures that aren't included in the programmes they are using, making firewalls and other security measures more vulnerable. We should look about the security concerns that these mobile enterprises face on a daily basis. In addition, because mobile enterprises are so prone to these kinds of digital crimes, extreme caution should be exercised in the case of a security breach.

4.5 IPv6: New web convention

New Internet protocol, IPv6, is replacing IPv4 (the previous version), which has been a backbone of our companies and Internet in general for many decades. IPv6 security isn't only a matter of bringing IPv4 capabilities over to IPv6. Although IPv6 is a cost-effective way to increase the number of IP addresses, there are a number of fundamental modifications to the standard that should be considered in a security policy. When practicable, it is best to use IPv6 whenever possible to reduce the danger of cyber attacks.

4.6 Encryption of the code

A prevalent way to make communications (or data) impenetrable to public scrutiny or programmers is through the use of encryption. By utilizing an encryption computation, the message or data is divided into a code text. The message is encoded using an encryption key, which specifies how it will be decoded. The confidentiality and integrity of data are ensured by encryption from the earliest possible point of reference. Increased use of encryption, on the other hand, exacerbates the problem of network security. To protect information while it travels, such as over networks (e.g. the Internet, e-commerce), cell phones (remote receivers, remote radios), etc., encryption is utilized. As a result, by encoding the code, one is aware if any data spills.

5.JOB OF SOCIAL MEDIA IN NETWORK PROTECTION

As people become more social in a more connected world, organizations should search for new ways to protect individual data. The role of social media in digital protection is enormous, and it will have a significant impact on individual digital risks. Risk of assault increases as the popularity of web-based entertainment at work grows. Since

so many individuals regularly access online entertainment and informal communication sites, it's become a great stage for digital fraudsters to access private data and steal crucial information. As we know it in the real world, we're fast to hand over our personal details, so companies need to ensure that they're just as quick to see risks, respond quickly, and avoid a breach of any kind. The programmers utilize these virtual entertainments as a trap to get the data and information they need since people are effectively attracted in by them.

In order to avoid a lack of data, individuals need take adequate precautions, especially when it comes to managing virtual entertainment.

Virtual entertainment offers companies with a unique set of challenges since it requires individuals to be able to exchange data with a large group of people. Additionally, internet entertainment provides a comparable potential to distribute fake data, which may be just as damaging as industrially sensitive information might be. The transmission of misleading info through online entertainment is one of the new threats highlighted in the 2013 Global Risks report.

No matter how it can be used to commit digital crimes, internet entertainment is a vital aspect of how an organization is revealed, thus these companies can stop using it. A mechanism that alerts them to a problem before any real harm is done should be in place, barring any unforeseen circumstances. It is critical for businesses to realise this and recognise the necessity of analyzing data, especially in amicable interactions, and to implement necessary measures to minimize risks. Virtual entertainment should be approached in a certain way and with the proper technological improvements in mind.

6. CYBER SECURITY TECHNIQUES

6.1 Access control and secret phrase security

Client names and secret phrases have been an important part of our approach to data security. This might be one of the early stages in the development of data security.

6.2 Authentication of information

In order to ensure that the reports we get are accurate, they should be reviewed for modifications before they are received from a reputable and dependable source. The anti-infection software on the devices is usually able to verify these reports. Similarly, anti-infection software is required to protect against infection on the devices.

6.3 Malware scanners

All files and archives on the system are examined for malicious code or destructive infections in the vast majority of cases. "Malware" refers to programmes like worms and Trojan horses that infect computers and are usually referred to as.

6.4 Firewalls

A firewall is software or hardware that prevents hackers, viruses, and worms from gaining access to your computer over the Internet. There is a firewall in place that examines each communication and blocks those that don't adhere to the specified security models before entering or leaving the web. As a consequence, firewalls are critical for detecting malicious code.

6.5 Anti-infection programming

One of the most important functions of a computer's operating system is the ability to detect and eliminate malicious code, such as worms and viruses. The auto-update feature in most antivirus packages allows the software to download updated infection profiles so that it can scan for new viruses as they are discovered. Each framework must have an anti-infection programme in order to work effectively.

7. CYBER ETHICS

The web's code is all there is to digital morals. If we follow certain computer ethics, we can utilize the internet in a legitimate and secure way. A few instances are given below:

- Use the Internet to stay in touch with friends and family. To stay in touch with loved ones, coworkers, and people all over the world by email or SMS is easier than ever before thanks to modern technology.
- On the internet, try not to be a domineering jerk. It is against the law to insult others by calling them by their names, lying about them, or sending them humiliating images.
- As the world's largest repository of information on practically any subject or field of study, the Internet must be used in a legal and ethical manner.
- Try not to use passwords from other people's accounts to access your own.
- Do not attempt to communicate malware to other frameworks in order to cause them to fail.
- There is a good chance that someone else may take advantage of your personal information, which might land you in a sticky scenario.
- When you're online, never pretend to be someone else or try to create a false identity for someone else since it might get you both into trouble.

- Maintain a strict adherence to protected data and only download games or recordings if the cost is reasonable.

The following are a few digital values that everybody must adhere to when using the web. From the outset, we've held ourselves to the same high standards that we do on the internet.

7. CONCLUSION

As the world gets more interconnected and networks are utilized to conduct everyday transactions, PC security has grown to be a major problem. Each New Year brings new avenues for cyber criminals, and as a result, so does the protection of data. The most recent and problematic developments, together with the new digital gadgets and dangers that emerge evident every day, are trying associations in terms of how they protect their foundation, yet the manner in which they demand new stages and expertise to do so is testing as such.. There is no one-size-fits-all solution to digital violations, but we should do our best to limit them in order to ensure a future free of possible harm on the internet.

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.