ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940 Vol 17, Issue 4, 2023
www.ijasem.org

An Analysis of Cybersecurity Challenges and Emerging Trends in Cutting-Edge Technologies

Mrs. TAHERA ABID[1], Mrs. NAZIA AMREEN[2], Ms. ZAHOORA ABID[3]
Department of Information technology
Nawab Shah Alam Khan College of Engineering and Technology

ABSTRACT

Cybersecurity is a big deal in the world of IT.The safety of information has become one of the most difficult issues these days. The first thing that comes to mind when we think about cyber security is "cyber crimes," which are becoming a lot more common every day. Many steps are being taken by governments and businesses to stop these online crimes. Even though there are many steps being taken, internet security is still a big issue for many. This essay is mostly about the problems that come up with internet security for new technologies.It also talks about the newest methods, ethics, and trends that are changing the way cyber security is done.

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

1. INTRODUCTION

With the click of a button, people can send and receive any kind of data these days, whether it's an email, an audio file, or a video file. But has anyone ever thought about how safely their data is being sent to the other person, without any information getting out? Cybersecurity is the key to the answer. These days, the Internet is the most rapidly expanding part of daily life. In today's high-tech world, many new tools are changing the way people live. Unfortunately, these new technologies make it harder for us to keep our private information safe. As a result, online crimes are on the rise every day. More than 60% of all business transactions happen online these days, so this area needs high levels of security to make sure transactions are clear and safe. This is why internet security is now a big deal. Cybersecurity isn't just about keeping information safe in the IT field; it also applies to many other areas, and not just the IT field.

We need to make sure that even the newest tools, like cloud computing, mobile computing, E-commerce, net banking, etc., are safe. Because these technologies hold important information about a person, they need to be kept safe at all times. Improving cyber security and keeping important information systems safe are important for every country's economic and security. Protecting Internet users and making the Internet safer have become important parts of the growth of new programs and policies made by the government. There needs to be a better and more thorough way to fight online crime. Since technology means can't stop crimes on their own, it is very important that law enforcement be able to successfully examine and punish online crime. To keep important data from getting lost, many countries and governments are putting strict rules on internet security today. Everyone needs to be taught about cyber security so they can protect themselves from the growing number of online crimes.

2. CYBER CRIME

A computer is usually used as the main tool for any illegal action that is called "cyber crime." The U.S. Department of Justice says that any illegal action that uses a computer to store proof is now considered a cyber crime. Cyber crimes, which are on the rise, include crimes that computers have made possible, like hacking into networks and spreading computer viruses. They also include computerised versions of crimes that already exist, like identity theft, stalking, bullying, and terrorism, which have become big problems for people and countries. Cyber crime is usually thought of as a crime done on a computer or the internet to steal someone's name, sell illegal goods, stalk people, or mess up business with bad intentions. to programs. Cybercrime will rise along with technological progress because technology is becoming more and more important in people's lives.

3. CYBER SECURITY

Privacy and security of the data will always be top security measures that any organization takes care. We are presently living in a world where all the information is maintained in a digital or a cyber form. Social networking sites provide a space where users feel safe as they interact with 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 but also during bank transactions a person must take all the required security measures. technology and healthcare executives nationwide, Silicon Valley Bank found that companies believe cyber attacks are a serious threat to both their data and their business continuity.

- 98% of companies are maintaining or increasing their cyber security resources and of those, half are increasing resources devoted to online attacks this year
- The majority of companies are preparing for when, not if, cyber attacks occur
- Only one-third are completely confident in the security of their information and even less confident about the security measures of their business partners.

There will be new attacks on Android operating system based devices, but it will not be on massive scale. The fact tablets share the same operating system as smart phones means they will be soon targeted by the same malware as those platforms. The number of malware specimens for Macs would continue to grow, though much less than in the case of PCs. Windows 8 will allow users to develop applications for virtually any device (PCs, tablets and smart phones) running Windows 8, so it will be possible to develop malicious applications like those for Android, hence these are some of the predicted trends in cyber security.

4. TRENDS CHANGING CYBER SECURITY

Here mentioned below are some of 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 attention of media, are also 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 data. Hence one must always use a safer browser especially during important transactions in order not to fall as a prey for these crimes.

4.2 Cloud computing and its services

These days all small, medium and large companies are slowly adopting cloud services. In other words the world is slowly moving towards the clouds. This latest trend presents a big challenge for cyber security, as traffic can go around traditional points of inspection. Additionally, 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. Though cloud services are developing their own models still a lot of issues are being brought up about their security. Cloud may provide immense opportunities but it should always be noted that as the cloud evolves so as its security concerns increase.

4.3 APT's and targeted attacks

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

4.4 Mobile Networks

Today we are able to connect to anyone in any part of the world. But for these mobile networks security is a very big concern. These days 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. We must always think about the security issues of these mobile networks. Further mobile networks are highly prone to these cyber crimes a lot of care must be taken in case of their security issues.

4.5 IPv6: New internet protocol

IPv6 is the new Internet protocol which is replacing IPv4 (the older version), which has been a backbone of our networks in general and the Internet at large. Protecting 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. Hence it is always better to switch to IPv6 as soon as possible in order to reduce the risks regarding cyber crime.

4.6 Encryption of the code

Encryption is 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 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. Encryption is also used to protect data in transit, for example data being transferred via networks (e.g. the Internet, e- commerce), mobile telephones, wireless microphones, wireless intercoms etc. Hence by encrypting the code one can know if there is any leakage 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.

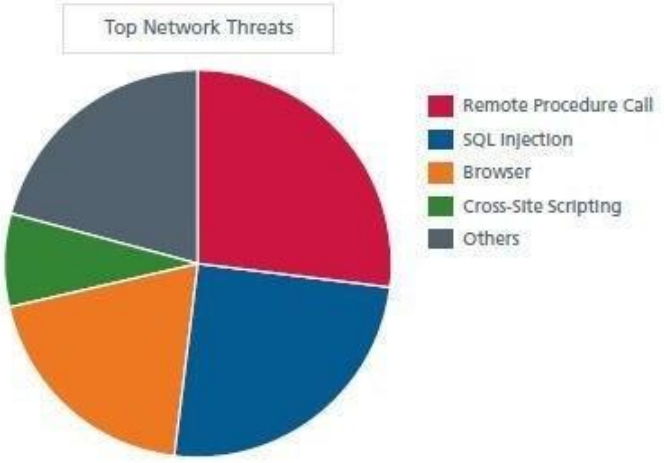

Fig -1 The above pie chart shows about the major threats for networks and cyber security.

5. ROLE OF SOCIAL MEDIA IN CYBER SECURITY

Companies need to come up with new ways to keep personal information safe as people become more social in a world that is becoming more linked. A lot of personal cyber risks will come from social media, which is a big part of cyber security. The number of employees using social media is through the roof, and so is the risk of attack. Being that most of them use social media or networking sites every day, it has become a big place for hackers to get private information and steal important data.

Companies need to be just as quick to spot risks, react in real time, and avoid any kind of breach in a world where people are quick to give up their personal information. Hackers use these social networks as bait to get the information and data they need because they are easy for people to get hooked on. Because of this, people need to take the right steps, especially when using social media, to keep their information safe.

In the heart of the problem that social media poses to companies lies the fact that anyone can share information with millions of people. On top of letting anyone share information that could be harmful to businesses, social media also lets anyone share fake information, which can be just as unhealthy. One of the new risks that the Global Risks 2013 study talks about is how quickly fake information can spread on social media.

Social media can be used for online crimes, but businesses can't stop using it because it helps them get known. Instead, they need ways to know about the threat so that they can fix it before it does any real damage. Companies should know this, though, and know how important it is to look at the information, especially in social talks, and come up with the right security measures to avoid risks. When using social media, you need to follow certain rules and use the right tools.

6. CYBER SECURITY TECHNIQUES

6.1 Access control and password security

The concept of user name and password has been fundamental way of protecting our information. This may be one of the first measures regarding cyber security.

6.2 Authentication of data

The documents that we receive must always be authenticated be before downloading that is it should be checked if it has originated from a trusted and a reliable source and that they are not altered. Authenticating of these documents is usually done by the anti virus software present in the devices. Thus a good anti virus software is also essential to protect the devices from viruses.

6.3 Malware scanners

This is software that 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.

6.4 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.

6.5 Anti-virus software

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. An anti virus software is a must and basic necessity for every system.

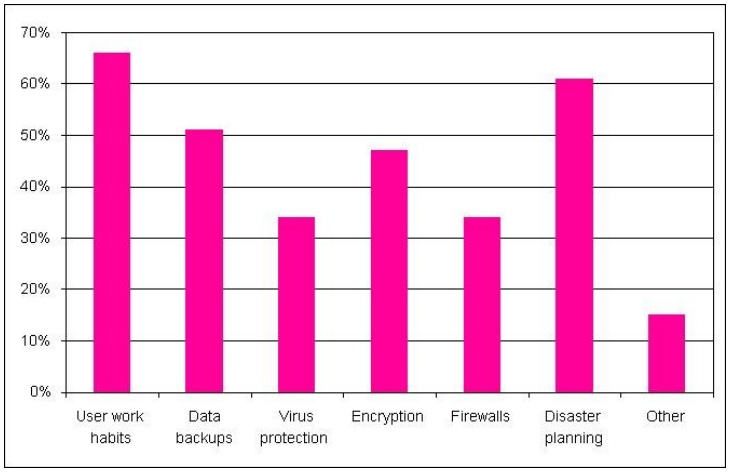

Table II: Techniques on cyber security

7. CYBER ETHICS

Cyber ethics are nothing but the code of the internet. When we practice these cyber ethics there are good chances of us using the internet in a proper and safer way. The below are a few of them:

- DO use the Internet to communicate and interact with other people. Email and instant messaging make it easy to stay in touch with friends and family members, communicate with work colleagues, and share ideas and information with people across town or halfway around the world
- 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.
- 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 try to send any kind of malware to other's systems and make them corrupt.
- 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.
- When you're online never pretend to the other person, and never try to create fake accounts on someone else as it would land you as well as the other person into trouble.
- Always adhere to copyrighted information and download games or videos only if they are permissible.

The above are a few cyber ethics one must follow while using the internet. We are always thought proper rules from out very early stages the same here we apply in cyber space.

8. CONCLUSION

Computer security is a big subject that is becoming more important as the world becomes more linked together and networks are used for important processes. With each new year, cyber crime goes in a different direction, and so does the safety of the information. Every day, new cyber tools and dangers appear along with the newest and most disruptive technologies. These are making it hard for businesses to keep their systems safe and needing new platforms and intelligence to do so. There is no perfect way to stop cyber crimes, but we should do everything we can to cut them down so that the future of cyberspace is safe and secure.

REFERENCES

1. A Sophos article 04.12v1.dNA by James Lyne called "Eight Trends That Are Changing Network Security."
2. Cybersecurity: Knowing How to Avoid Cyber Crimes by Sunit Belapure Nineteen Godbole report is called Computer Security Practices in Non-Profit Organisations and was written by Audrie Krause.
3. Luis Corrons wrote "A Look Back on Cybersecurity 2012" for Panda Labs.

4. "Study of Cloud Computing in the HealthCare Industry" by G.Nikhita Reddy and G.J.Ugander Reddy was published in the International Journal of Scientific & Engineering Research, Volume 4,
5. Issue 9, September 2013, Pages 68–71. The journal's ISSN number is 2229-5518.
6. IEEE Security and Privacy Magazine – IEEECS "Safety Critical Systems – Next Generation" July/August 2013.
7. Cybersecurity in Malasia by Avanthi Kumar in CIO Asia, September 3, H1 2013.