WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

Analysis of Cyber Security Challenges and the Most Up-To-Date Technologies

Md Maaz Ali[1], Masshood Siddiqui[2]

[1]MTech Scholar, Computer Science & Engineering Deptt, Bhabha University, Bhopal
[2]Assistant Professor, Computer Science & Engineering Deptt, Bhabha University, Bhopal

ABSTRACT :

Cyber security plays an important role in the field of information technology, information security has become one of the greatest challenges of our time. When we think of cybersecurity, we first think of cybercrime, which is on the rise. Many governments and companies are taking many steps to prevent this cybercrime. In addition to various measures, cybersecurity is still a major concern. This article mainly focuses on the cybersecurity challenges with the latest technologies, as well as the latest technologies, ethics, and cybersecurity trends that are changing the face of cybersecurity.

INTRODUCTION

Nowadays people can send and receive any kind of data like email, audio or video with just one click, but have you ever thought about sending a badge or seamlessly securing it to someone else? ? The answer lies in cybersecurity. Today, the Internet is the fastest growing infrastructure in everyday life. In today's technical environment, many modern technologies are changing the human face. But because of these emerging technologies, we cannot protect our private information very effectively, which is why cybercrime is on the rise. Today more than 60% of all business transactions are carried out online, so this area requires a high level of security for the most transparent and best transactions. Therefore, cybersecurity has become a modern issue. The scope of cybersecurity includes not only information security in the IT industry, but also in many other areas such as cyberspace and so on. Because these technologies contain vital information about a person, their safety is essential. Strengthening cybersecurity and protecting the information infrastructure are critical to the security and economic well-being of any country. Internet security (and protecting Internet users) has become an integral part of new service development and government policy. Tackling cybercrime requires a broader and safer approach. Since technical measures alone cannot prevent crime, it is important that law enforcement agencies are able to effectively investigate and prosecute cybercrime. Many countries and governments today impose strict laws on electronic securities to prevent the loss of important information. Everyone should be trained in cybersecurity and protect themselves from this growing cybercrime.

CYBER CRIME

Internet crime is a term for any illegal activity that the computer uses as a basic factor for the commission and theft. The US Department of Justice defines Internet crimes expanding illegal activities that a computer used to store evidence. The growing electronic crime list includes crimes involved by the computer, including the network of installation and deployment of computer viruses, as well as computer-based changes in current crimes, such as identity, pursuit, bullying and terrorism that they become a big problem for People and nation. An electronic crime in an electronic language in common language as a crime has been committed to using a computer and Internet identity of steel or sale of telegrams, vacation victims or disabling processes with malicious programs. While today's technology plays a major role in the life of a person, Internet crimes will increase with technology advancement.

CYBER SECURITY :

Data protection and security always have the highest security standards that are important to every organization. Today we live in a world in which all information is stored digitally or electronically. Social media provides a space in which users can feel safe communicating with friends and family. In the case of home users, cyber criminals continue to target social media sites to steal personal information. Not only in social networks, but also in banking, you have to take all the necessary security precautions.

TRENDS CHANGING CYBER SECURITY :

Web servers :

The threat of attacking web applications to extract data or distribute malicious code remains. Cyber criminals spread their malicious code through legitimate hacked web servers. Information theft attacks, many of which have caught media attention, are also a major threat. We now need to focus more on protecting web servers and web applications. Web servers in particular are the best platform for information theft by these cyber criminals. Therefore, especially with important transactions, it is always necessary to use a more secure browser to avoid falling into the trap of these crimes.

Cloud computing and its services:

Today, all small, medium and large businesses are slowly starting to use cloud services. In other words, the world is slowly moving towards the clouds. This recent trend poses a major cybersecurity challenge as traffic can move through traditional inspection centers. In addition, as the number of applications in the cloud increases, so do the guidelines for web applications and cloud services to prevent the loss of valuable information. Although cloud services have developed their own models, there are still many questions about their security. The cloud can offer tremendous opportunities, but it should always be kept in mind that as the cloud evolves, security concerns also increase.

APT's and targeted attacks :

APT (Continuous Advanced Threat) is a tool for a new level of cyber crime. Network security functions such as web filtering or IPS have played an important role in the detection of such targeted attacks (often after the first hack) for years. As attackers become more adventurous and use vague techniques, network security must be integrated with other security services in order to detect attacks. Therefore, we need to upgrade our security technologies to prevent further threats in the future.

Mobile Networks :

Today we can call anyone anywhere in the world. But for these cellular networks, security is a major concern. Firewalls and other security measures are now pervasive because people use devices like tablets, phones, computers, etc., all of which in turn require more security than those used in applications. We always have to think about the security problems of these cellular networks. More and more cellular networks are very vulnerable to this cybercrime, and more caution should be exercised in the event of a security breach.

IPv6: New internet protocol :

IPv6 is the new internet protocol replacing IPv4 (the old version) which is the backbone of our networks in general and the internet in general. IPv6 protection is not just about broadcasting IPv4 functions. Although IPv6 is an important alternative to providing more IP addresses, there are some fundamental changes to the protocol that need to be considered in the security policy. Therefore, it is always best to switch to IPv6 as soon as possible to reduce the risk of cybercrime.

Encryption of the code :

Encryption is the process of encrypting messages (or information) so that eavesdroppers or hackers cannot read them. In an encryption scheme, messages or information are encrypted using an encryption algorithm, which turns them into illegible ciphertext. This is usually done using the encryption key, which determines how the message is encrypted. The encryption primarily protects data protection and integrity. But the increasing use of encryption poses additional challenges for cybersecurity. Encryption is also used to protect the data sent, for example data sent over the network (such as the Internet and e-commerce), cell phones, wireless microphones, wireless intercoms, etc. In the event of data leakage.

ROLE OF SOCIAL MEDIA IN CYBER SECURITY:

As we are in a growing social population, companies should find new ways to protect personal information. Social resources play an important role in cyber safety and will greatly help personalized Internet threats. The adoption of social media under employees increases and therefore the threat of attack. Since social media or social networking sites are almost daily almost daily, a large platform for cyber systems for penetrating specific information and theft of value information. In the world we are sincerely, we need to leave your personal information, companies should quickly take care of the threats and real-time response and support any violations of any. Because people can easily be absorbed using these social media, hackers use as a restaurant for information and information they need. Therefore, people should take certain actions in dealing with social media to prevent loss of their information. The ability of individuals to share information with millions of millions in the heart is special challenges that provide social media. In addition to giving anyone able to distribute sensitive business information, social media also provide similar energy to expand false information that can only be harmful. The rapid distribution of incorrect information through social media is one of

the emerging dangers, in the global report of the 2013 World Report, but social media can be used for cybercrime, companies can not use social media because they Plays an important role in the company. Instead, they should have solutions that inform you that they will repair them before they get a real injury. However, companies must understand this and confirm the importance of analyzing information, especially in social dialogue, and provide appropriate security solutions for risk transfer. We must deal with social media with specific policies and technologies.

CYBER SECURITY TECHNIQUES :

- Malware scanners are programs that typically scan all files and documents in the system for malicious code or viruses. Viruses, worms, and Trojan horses are examples of malware that is often grouped together and referred to as malware.

- Firewall A firewall is software or hardware that prevents hackers, viruses, and worms from trying to access your computer over the Internet. All incoming or outgoing Internet messages pass through an existing firewall that monitors every message and blocks messages that do not meet certain security standards. Therefore, firewalls play an important role in the detection of malware.

- Anti-virus software An anti-virus program is a computer program that detects, prevents, and removes or removes malware, such as viruses and worms. Most anti-virus software includes an automatic update feature that allows the software to download new virus definition files so that it can check for new viruses as soon as they are detected. Antivirus software is an essential requirement for any system.

- Access control and password protection The concept of the username and password is an essential way to protect our information. This can be one of the first steps in cybersecurity.

- Data authentication The documents we receive before they are downloaded must always be verified, so make sure they are from a reputable source and have not been modified. These documents are usually checked by the antivirus software on the devices. Hence, a good antivirus is essential to keep your devices safe from viruses.

CYBER ETHICS

Internet ethics is nothing more than an internet blog. If we apply these internet ethics, there are good ways to use the internet in a safe and appropriate manner. Here are a few:

Use the internet to communicate with and connect with others. Email and instant messaging allow you to keep in touch with friends and family, connect with colleagues, and share your ideas and information with people in the city or around the world. but Don't be a bully online. Don't call people's names, lie to them, send them embarrassing photos, or do anything else that could harm them. The Internet is the largest library in the world that contains information on any subject in any field, so it is always necessary to use this information correctly and legally. Accounts Don't use other people's accounts with your passwords. Never try to send malware onto someone else's system in order to harm them. Never give your personal information to third parties, as others could misuse them and you could get into trouble. When online, never pretend to be the other party and never try to create a fake account with someone else as it will cause problems for you and the other party. Always stick to copyrighted information and only download games or videos when allowed. Here are some electronic principles that you must follow when using the Internet. We always think that the rules are the same from the start that we apply here in cyberspace.

CONCLUSION

Computer security is a broad topic that is becoming increasingly important as the world becomes increasingly connected and uses networks for important transactions. Also in the new year, cybercrime differs in different directions and information security. The latest intrusive technologies as well as new cyber tools and new threats present companies not only with the challenge of protecting their infrastructure, but also of how they need new platforms and information to do so. There is no perfect solution to cybercrime, but we must do our best to reduce it in order to have a secure future in cyberspace.

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.