Overview of Cyber Crime and Cyber Security

Rajeev Sharma, Department Of Computer Science and Engineering
Galgotias University, Yamuna Expressway Greater Noida, Uttar Pradesh
E-mail id – not provided

ABSTRACT: In the field of information technology, cyber security plays an important role. Securing information has become one of today's biggest challenges. The first thing that comes to our mind when we ever think of cyber security is 'cyber crimes,' which are increasing immensely every day. Various governments and companies are taking a number of measures to prevent this from happening. Cyberdelinquency. Cyber protection is also a very major problem for us beyond different initiatives. This paper focuses mainly on information security issues on the new technology. It also reflects on the current cyber security strategies, practices, and developments that transform the face of cyber security.

Keywords: Cyber Security, Cyber Crime, Cyber Ethics, Social Media, Cloud Computing, Android Apps.

INTRODUCTION

Today man can send and receive some type of data may be an e-mail or an audio or video only by clicking a button but has he ever considered how easily his data I d is transferred or sent to the other person safely without any information leakage?? The solution to that is cyber protection. Today the Internet is the most growing daily network. In the scientific light of today Environment Other new developments alter the man-like profile. But when we are unable to secure our private information in a very successful manner due to these new technology, cyber attacks are through day by day. More than 60 per cent of overall commercial transactions are carried out online today [1] and this area demanded a high degree of Security standard for transactions which are straightforward and highest.

Cyber protection has therefore become a most recent problem. The application of cyber security is not restricted to protecting information in the IT sector, but is also restricted to many other areas such as cyber space, etc. E-commerce, net banking and so forth often need a high degree of protection. As these technologies contain some valuable knowledge about a individual their protection has become a must. Improving data protection and safeguarding sensitive information infrastructures are key O The security and economic welfare of a country. Keeping the Web more accessible (and protecting Internet users) has been central to the advancement of emerging technology Loss some valuable pieces of knowledge. All really needs to be focused on this information protection to save themselves from these rising cyber criminals Loss some valuable pieces of knowledge. All really needs to be focused on this information protection to save themselves from these rising cyber criminals [2].

CYBER CRIME

Today man can send and receive some type of data may be an e-mail or an audio or video only by clicking a button but has he ever considered how easily his data I d is transferred or sent to the other person safely without any information leakage?? The solution to that is cyber protection. Today the Internet is the most growing daily network. In the scientific light of today Loss some valuable pieces of knowledge. All really needs to be focused on this information protection to save themselves from these rising cyber criminals Stalk victims or hinder malevolent activity Schedules. As day-to-day technology plays a significant role in the life of a human, cyber criminals will also increase along with advancements in technology [3].

CYBER SECURITY

Data protection and confidentiality should also be top security controls that are taken care of by every company. We now live in a world where all of the information is stored in a physical or cyber shape. Social networking sites offer a space where people feel safe when communicating with family and friends. Cyber-criminals will continue to strike socially in the case of home users Media sites are used to access confidential information. Not only social networking but even a individual must take all the appropriate security precautions during bank transactions.

SECURITY FEATURES

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

Web servers

The threat of software apps targeting data retrieval or spreading malicious code continues. Cyber criminals spread their malicious code via legal, hacked web servers. But data-stealing attacks are still a major threat, many of which get media coverage. Now, more emphasis is needed on protecting web servers and web applications. Web servers in particular provide these cyber criminals with the best place to steal the data. Therefore, in order not to fall as a victim for such crimes, one must always use a safer browser particularly during important transactions [4].

Cloud computing and its services

Today cloud platforms are increasingly being embraced by both small, medium and big businesses [5]. In other words the atmosphere is heading gradually into the clouds. This new phenomenon poses a big challenge for information defense, as traffic will wander conventional inspection points. In fact, If the number of cloud-accessible applications grows, regulatory frameworks for web apps and cloud providers will also need to change to avoid the loss of useful data. While cloud providers are creating their own models, many questions about their security are still being addressed. Cloud can bring enormous possibilities, but should always do so This should be remembered that the cloud is changing and its security issues are growing [6].

APT's and targeted attacks

APT (Advanced Persistent Threat) is a whole new type of warehousing organized crime. Network security features such as site filtering or IPS have been instrumental in detecting such targeted attacks for years (mostly after the initial compromise). When attackers are more brazen and use ambiguous tactics, network security has to be combined with other security services. To track bombardment. Therefore, our monitoring procedures must be strengthened to deter more attacks in the future

Mobile Networks

Today we in every area of the world are able to communicate with others. Security is therefore a very major issue for these cell networks. These days, firewalls and other security mechanisms are becoming vulnerable as people use apps such as laptops, computers, PCs, etc., all of which require external protections beyond those found in the software used. We still have to worry around the # Certain cell network stability issues. Further cell networks are particularly vulnerable to these cyber attacks and great caution must be taken in the event of their security problems [7].

IPv6: New internet protocol

IPv6 is the latest Internet protocol to replace IPv4 (the previous version), which became the foundation of our networks in general and of the Internet in general. Protecting IPv6 is not just about porting functionality to IPv4. Although IPv6 is a wholesale substitute for more IP addresses, there are some very basic protocol improvements that need to be madeTo be taken into consideration in safety policy. Therefore, upgrading to IPv6 as early as possible is often safer in order to reduce cyber security threats [8].

Encryption of the code

IPv6 is the latest Internet protocol to replace IPv4 (the previous version), which became the foundation of our networks in general and of the Internet in general. Protecting IPv6 is not just about porting functionality to IPv4. Although IPv6 is a wholesale substitute for more IP addresses, there are some very basic protocol improvements that need to be made Encryption at a very early level protects privacy and integrity of the data. Yet the use of encryption carries with it additional information security issues. Encryption is often used to encrypt transport data, such as data exchanged across networks (e.g. twitter, ecommerce), cell phones, wireless microphones, wireless intercoms, etc.

Role of Social Media In Cyber Security

When we become more mobile in an increasingly wired environment, companies need to consider new ways of securing personal information. Social networking is a big part of information security and internal cyber-attacks should add a lot. Adoption of social media by workers is skyrocketing and so is the possibility of an assault. It has become a major forum for cyber criminals to access private information and steal sensitive data because the social media or social networking sites are almost used by most of them every day [9].

Cyber Security Techniques

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

Authentication of data

The documents that we receive must always be authenticated be before downloading that is it It should be checked that it originates from a trustworthy and credible source, and that it is not changed. The authentication of these documents normally takes place via the anti-virus applications installed in the computers. A good anti-virus software is thus also essential to protect the devices against viruses.

Malware scanners

This is program that typically checks all the files and records for malicious code or dangerous viruses found in the network. Viruses, worms and trojan horses are examples of malware which is mostly grouped together and called malware

Firewalls

A firewall is a software system or hardware component that helps track hackers, malware, and worms attempting to get to your machine over the Internet. All messages that enter or exit the internet are transmitted through the present firewall, which analyses any message and blocks any that do not fit the defined security requirements. Firewalls also play an significant part in stopping the ‘malware' [10].

Anti-virus software

Antivirus software is a computer system that detects, stops, and works to disable or kill malicious software programs such as viruses and worms. Many antivirus applications have an auto-update feature that allows the system to import new virus profiles so that new viruses can be tested as soon as they are detected. Antivirus protection is a must and a clear requirement. Antivirus software is a computer system that detects, stops, and works to disable or kill malicious software programs such as viruses and worms. Many antivirus applications have an auto-update feature that allows the system to import new virus profiles so that new viruses can be tested as soon as they are detected. Antivirus protection is a must and a clear requirement.

Cyber Ethics

Cyber-ethics is nothing but the internet language. When we exercise this cyber ethic there are strong odds that we can access the internet correctly and safely. The ones below are just a few**:**

- 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.

Problematic Elements of Cyber Security

Security threats are one of the most troublesome aspects of information security. The conventional strategy concentrated most of the attention on the most critical components of the network and on defending against attacks, which necessitated keeping some of the less essential components of the network undefended and some of the less valuable dangers, i.e. not secured. In the present climate, such a method is inadequate.

MAJOR SECURITY PROBLEMS

Virus

A Virus is a program that is loaded to your machine without your knowledge and runs against your wishes. They are computer programs that bind themselves to or corrupt the machine or files which appear to circulate to other machines on the network by clicking on them, by fax, by mobile devices, etc. They interrupt the operation of the machine and affect the data stored either by changing it or by deleting it entirely. Definition of viruses: (1) Melissa, (2) Sasser, (3) Zeus, (4) Conficker, (5) Stuxnet, (6) Mydoom, (7) Red Code.

Warms

Worms, unlike viruses, do not require a host to cling to. They're only replicating until they've used up all the resources left on the machine. The word "worm" is often used to mean "self-replicating" malware (MALicious softWARE). It has some free memory of drives or other computers.Example of heat: (1) Badtrans, (2) Bagle, (3) Gun, (4) ExploreZip, (5) Kak worm, (6) Netsky, (7) SQL Slamme

Hacker

A rising hacker is a person who breaks into computers, usually by obtaining access to administrative controls.

White hat hacker

A white hat hacker is a information security expert who hacks into secure systems and networks to check and determine their protection. White hat hackers use their expertise to boost security by revealing bugs to malicious hackers (known as black hat hackers) who can identify and manipulate them.While the methods used are similar, if not equivalent, to those used, Malicious hackers, white hat hackers, have permission to recruit them against the company that recruited them.

Grey Hat Hacker

The word "white hat" or "blue hat" applies to a computer hacker or information security specialist who can often break the law or traditional ethical norms, but who has no criminal intent characteristic of a black hat hacker.

Black Hat Hacker

A black hat hacker is a person with advanced computer skills whose aim is to break or circumvent Internet security. Black hat hackers are also known as crackers or dark-sided hackers. The general opinion is that while hackers are constructing stuff, crackers are smashing things.

CONCLUSION

Computer security is a vast issue that is becoming more and more important because the world is becoming highly interconnected and networks are being used to carry out critical transactions. Every New Year that passes, and so does the security of information, cyber crime continues to diverge along different paths. The latest and disruptive technologies, along with new cyber tools and threats,

REFERENCES

[1] R. Von Solms and J. Van Niekerk, “From information security to cyber security,” *Comput. Secur.*, 2013, doi: 10.1016/j.cose.2013.04.004.

[2] M. Sonntag, “Cyber security,” in *IDIMT 2016 - Information Technology, Society and Economy Strategic Cross-Influences - 24th Interdisciplinary Information Management Talks*, 2016, doi: 10.2478/hjbpa-2019-0020.

[3] A. L. Buczak and E. Guven, “A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection,” *IEEE Commun. Surv. Tutorials*, 2016, doi: 10.1109/COMST.2015.2494502.

[4] U. Franke and J. Brynielsson, “Cyber situational awareness - A systematic review of the literature,” *Computers and Security*. 2014, doi: 10.1016/j.cose.2014.06.008.

[5] M. Robinson, K. Jones, and H. Janicke, “Cyber warfare: Issues and challenges,” *Comput. Secur.*, 2015, doi: 10.1016/j.cose.2014.11.007.

[6] A. Humayed, J. Lin, F. Li, and B. Luo, “Cyber-Physical Systems Security - A Survey,” *IEEE Internet Things J.*, 2017, doi: 10.1109/JIOT.2017.2703172.

[7] Homeland Security, “Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies,” *Ics-Cert*, 2016.

[8] N. Choucri, S. Madnick, and J. Ferwerda, “Institutions for Cyber Security: International Responses and Global Imperatives,” *Inf. Technol. Dev.*, 2014, doi: 10.1080/02681102.2013.836699.

[9] J. Srinivas, A. K. Das, and N. Kumar, “Government regulations in cyber security: Framework, standards and recommendations,” *Futur. Gener. Comput. Syst.*, 2019, doi: 10.1016/j.future.2018.09.063.

[10] A. Verma, “Cyber pornography in India and its implication on cyber café operators,” *Comput. Law Secur. Rev.*, 2012, doi: 10.1016/j.clsr.2011.11.003.

.