DOI-10.53571/NJESR.2020.2.4.6-14

Cyber Security Challenges And its Emerging Trends On Latest Technologies

Meha Khiria
Assistant Professor
School Of Law
M.G.S.University
Bikaner

(Received:29March2020/Revised:10April2020/Accepted:20April 2020/Published:30April2020)

Abstract

Today, due to the modern life style people have joined technology life and using more technology for shopping as well as financial transactions in their cyber space. At the same time safeguarding of knowledge has become increasingly difficult. In addition, the heavy use and growth of social media, online crime or cybercrime has increased. In the world of information technology, data security plays a significant role. The information security has become one of today's main challenges. Whenever we think of cyber security, we first of all think of 'cybercrimes,' which expand tremendously every day. Different government and businesses take various steps to avoid this form of cybercrime. In addition to numerous cyber protection initiatives, many people are also very worried about it. This paper focuses primarily on cyber security concerns related to the new technology. It also concentrates on the new technologies for cyber security, ethics and developments that impact cyber security.

Keywords: Cyber security, Cybercrime, Android apps, Social networks,

Introduction

The process of digitization in all aspects of human life, like healthcare, education, business, etc.,has gradually led to the storage of all sorts of information, including sensitive data. Security is the process of protecting the digitized information from theft or from physical damage while maintaining the confidentiality and availability of information but as technology is growing rapidly, the cybercrime rate also increases both in number and complexity. The reason behind this tremendous growth in cyber-crime is the usage of inadequate software, expired security tools, design flaws, programming errors, easily available online hacking tools, lack of awareness in public, high rates of financial returns, etc. In order to explore the vulnerabilities in the target and thereby to attack the victim, more powerful attack tools are developed by the technical attackers. With this, new attacks in different variations are coming which are difficult to detect. Increase in internet dependency in all walks of life, digital nature of data in huge amounts getting accumulated through online transactions and decentralization of data repositories, has led to the development of effective security algorithms. The continuously changing nature of cybercrime also leads to the difficulty of handling and avoiding emerging threats. The task of securing cyber-space is the most difficult and challenging task as advanced threats play a very active role. Therefore, it is necessary to get insights into the concepts of security defense mechanisms, different techniques and trending topics in the area of information security

Cyber Crime

Cybercrime is a term for a crime which uses a PC for robbery and crime of commission. The United States Department of Justice has extended the scope of cybercrime to cover any crime that uses a device for evidence storage. The increasing list of cybercrimes includes computer crimes, such as the spread of network intrusions and pc-viruses, as well as the computer-based variant of established crimes such as theft, stalking, intimidation, and coercion. Often cyber-crimes in common people's language may also be defined as crimes committed using a PC and the web to steal the identity or sell an individual to victims of smuggling or stalking or disrupting operations with malicious programme. As technology has a major role in the lives of an extremely individual day by day, cybercrimes too can increase alongside technological advancements.

Cyber Security

Privacy and information protection can be the primary security behaviour which any company cares about continually. We prefer to square measurements currently in a highly digital or cyber-specific environment in which all the data are stored. Social networking sites provide an environment wherever users feel secure while they function with friends and family, cyber criminals also seek to steal personal information via social media sites.

Scope of The Study

The interactive structure of the financial environment will be a direct impact on one aspect of the institution's infrastructure and the sensibilities of the financial sector to cybercrimes, in particular attacks on Denial-of-Services. In order to secure all the confidential information from falling into wrong hands, the finance sector should continually track and innovate its systems. The banking sector has always been the leading player in implementing safety systems and behavior and has also been the leading cyber security investment sector.

Literature Review

Julian Jang-Jaccard [1] Improving cyber security and protecting critical information infrastructure is important for the security and economic well-being of each country. Safer Internet (and protecting Internet users) have been an important part of the growth of new services and public policy.

Lee, H.; Lee, et al [2]. Various attachment methods have emerged in the past and the key logger is a representative attack tool, which records all user's keyboard data entries and can be easily obtained from the Internet.

Mellado, D.; Mouratidis et al,[3]. Protection is an area in the SPL that has not been studied. Most methods concentrate on implementing safety criteria or properties in the SPL. There were various approaches to variability management and safety criteria from the early stages of production of the product line.

Mohsin, M.; Anwar et al, [4] Whether the established techniques of feature models can be implemented or adapted for cyber security is the challenge in the fields of cyber security. In an approach is proposed in order to enhance the production and the derivative products of safe software product lines (SPLs).

VeenooUpadhyay [5] The wizard asks the user to add "labels" of privacy to select friends, and he uses this feedback to create a classifier using the machine learning pattern, which can be used to allocate privileges to the other user friends automatically. The insight for the design stems from the observation that actual users understand their privacy habits and that friend can see which details they use and reproduce in other friends' settings, based on an implicit set of rules.

Yim, K [6]The main principle of this technique prevents the user from disclosing the actual keyboard data entrance but detects the keyboard data attack techniques. In particular, by producing the random keyboard data, the defender calls for a keyboard input event to secure the user 's actual keyboard data intake by filtering the keyboard data generation.

Nikita TresaCyriacLipsaSadath [7]The paper also discusses the perpetrators of a cyber-attack and the techniques primarily used to achieve their goal. It sheds light on the overall structure of cyber- assault and on its phases and its impact on the financial system.

MdLiakat Ali [8] This study presents a brief overview of the cyber security problems raised by modern developments in technology and innovations; the paper is also focused on the latest cyber security strategies, trends and other ethics in cyber security.

Kutub Thakur [9]Cyber security was used interchangeably for the security of knowledge, where later it sees the human's role in the safety process, although formerly finding this an additional dimension. However, such a debate on cyber safety has major consequences, since it reflects on the ethical part of the whole society. Various systems and models have been developed to solve the problem of cyber security.

J.li [10] Evaluated firewalls issues and how the routing tables can be configured in a way that minimizes the maximized firewall rule set which helps to avoid performance bottlenecks and limit safety breakthroughs. The problems are NP-full and an heuristic approach has been suggested to demonstrate the efficacy of algorithms using simulations. Two major contributions have also taken place.

Cyber Security Techniques

Cyber-attacks on cyberspace can grow by capitalizing on new techniques. Cybercriminals will most frequently change the current malware signatures to take advantage of new technical faults. In other instances, they actually search for special features of emerging technology to detect weaknesses in malware injection. Cyber criminals are taking advantage of emerging Internet technology and millions and billions of active users to access a huge amount of people easily and effectively using these new technologies.

Access Control and Password Security

Security provided by the means of username and password is a simple way of providing security for the private information to preserve privacy. This means of providing security is one of the most critical cyber security initiatives.

Authentication of Data

Until the transmitted information need to be attested that it has come from a reputable supply that was not changed. These documents are often authenticated using a gift from the opposing virus software package inside computers. An honestly opposed virus software package is more essential to protect devices from viruses.

Malware Scanners

A software system which sometimes scans all files and documents for malicious code or harmful viruses inside the system. The samples of malicious software systems in this field are generally sortingand noted as malware by viruses, worms, and the Trojan horses.

Firewall

Firewall is a software or hardware package which helps separate hackers, viruses and worms trying to access your PC through the web .The firewall checks all messages that come in and blocks those that fail to meet the security requirements compatible with all messages .Firewalls plays a very vital role in malware detection.

Role of Social Media in Cyber Security

In recent modern world, there is a need of interactive businesses which needs to find new ways to secure personal information in more entangled environment. Social media has important role to play in cyber security and in personal cyber-attacks. Adoption of social media among employees is growing and threat of attack is therefore increasing since most of them nearly use social media or social networking sites everyday it is now a massive forum for cyber criminals to hack private information and steal valued information. In recent days, it’s very easy to share personal information easily and businesses must make sure that recognise, react in real time and prevent breaches of any kind as quickly as possible. These social media has easily make people to share their private information and hackers can use these information .therefore; people have to take reasonable steps to avoid misuse and loss of their information through these social media.

Recent Survey Issues on Cyber Security Trends

Cyber Security concerns the awareness concerning various cyber threats and the implementation of defense policies (i.e countermeasures) to safeguard confidentiality, credibility and availability of digital or IT technologies.

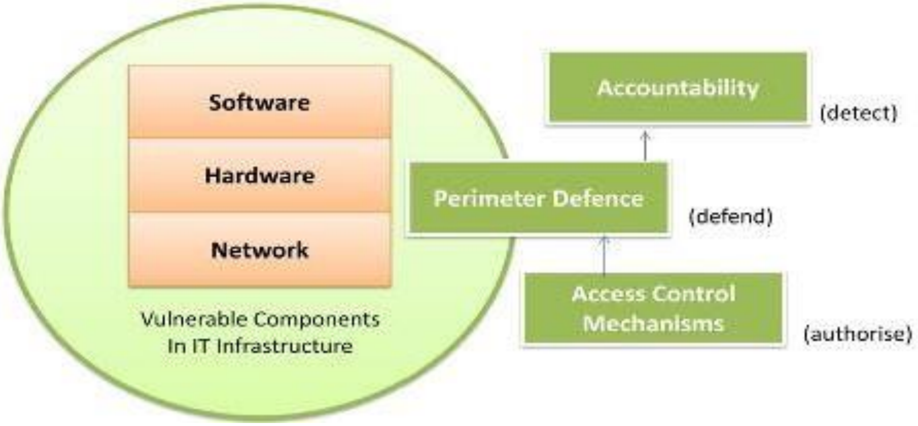

Fig 1: Vulnerabilities And Defense Strategies In Existing Systems

Many cyber security experts consider Malware is the main option for malicious arms to violate the cyber protection efforts of cyberspace. Malware is the widespread class of attacks loaded upon a device, generally without the knowledge of the rightful owner. Like viruses, worms, Trojan horses, spyware and bot executable, malware infects computers in several ways for example propagating from infected devices, trick users into opening tactile file or enticing users to visit websites of malware spreading. Malware could load itself into a USB drive inserted into an infected computer in more concrete cases of malware infection, and then infect any machine into which the computer is then inserted. Malware can spread from the embedded systems and computational logic of devices and equipment. Malware can be introduced in the device life cycle at any time. The victim of malware may vary from end-users, servers and network devices (e.g. routers, switching, etc.) to process control systems like the SCADA. The increase in the number of malware and its complexity are today a major concern in the Internet.

Phishing Attacks

According to Verizon's latest data violation survey, 32% of the data violations confirmed were attributable to phenomena. The purpose of the assaults is to collect confidential information such as usernames, passwords, the social security numbers and card details by duplicating the victims into believing they connect with a trustworthy person, by either email or by text, and increasingly by means of telephone.

IoTRansomware

The internet of things contains several devices, i.e. home equipment and service sensors, which are connected to the network. Climate control devices and refrigerators do not often contain confidential information through their own devices; they may be kept as hostages and are possible targets for hackers to access information in backend systems such as those in power supplies and communication facilities.

Increased Data Privacy Regulation

The General Data Protection Regulations for Europe (GDPR) was introduced in May 2018 to strengthen European citizens' rights of data privacy and to implement compliance with more rigorous global regulations or severe financial penalties for non-compliance.

Cyber Attacks on Mobile Devices

Recent RSA research has concluded that in 2018 " 80% of fraudulent mobile transactions " have risen exponentially with mobile app fraud since 2015 with mobile devices touching each part of our life and working life ,their risk perceptions also grow higher.

Increased Investment in Automation

Automation technology is gaining ground in organisations by allowing underemployed cyber security teams to focus on more complex problems, not on routine, often worldly work .According to a recent Ponemon Institute survey, 79% of respondents use security automation tools and frameworks and 50% expect to use security automation in their businesses. In these situations, the first approach to data protection provides an ultimate defense against Cyber-attacks such as database fraud and fitness, and its profound effect on a business .It may enhance efficiency, but skills and expertise are still necessary to minimize cyber security risk.

Preventive Measures To Avoid CyberCrimes

The five latest emerging trends in cyber security

1.Cyber security skills and organizations are also changing.

2.Protection in the cloud is a top priority.

3.Shift your attention from security and prevention

4.Production centers manage the application and data protection.

Next generation safety digital environments can only determine cybercrime through technological measures; capacity building, organizational structure and global collaboration, along with legislative steps, were also required

Conclusion

This paper concludes that the cyber-crime has significant consequences for national and economic security. It is pervasive, violent, ubiquitous and increasingly sophisticated. There are significant risks for many industry agencies, public and private organization's (especially critical infrastructure) for companies and governments alike, it will be necessary for future growth, innovation and competitive advantage to have a cyber-security role in all its components. Every New Year, the security of data, continues to differ from cybercrime by entirely different methods. The newest and most turbulent innovations, along with emerging cyber techniques and regular attacks, are difficult organisations that not only protect their infrastructure but also need new channels and intelligence. However, we do have to do our hardest to attenuate cybercrime so that we can have a healthy and stable future in cyber- houses. The technologies of stable Internet and efficient systems of the next century have been proposed as important research fields for the future. The advancement of global identity management and monitoring techniques to monitor opponents have also become an important issue in the future.

The enormous increase in Internet access and the progress of Internet-enabled devices, the rising numbers of the population and wide spread use of the Internet, frequently showing highly sensitive personal data with little realization of the implications of information leakage.

- We speculate that concerns relating to end user confidentiality will rise in line with the increasing amount of knowledge accessible on the internet in the future.
- Furthermore, usability issues are becoming ever more relevant as a way of intuitively learning

about and using end-user-oriented protection mechanisms without complicating
or profound learning curves to secure the data. Cyber safety practice in the community is built up with innovative patches that rectify existing security and confidentiality problems and move on to them.

- Some believe that this revolutionary strategy has failed and will be unable to fulfill future requirements, because the original Internet has been invented in a somewhat different context from how it is used today. An approach to "thinking beyond" is suggested to make better use of the increasingly-demands of the future without referring to the existing computing system and future, but to start again.

References

[1]Ravi Sharma Study of Latest Emerging Trends on Cyber Security and its challenges to Society International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012 1ISSN 2229-5518.

[2]Lee, H.; Lee, Y.; Lee, K.; Yim, K. Security Assessment on the Mouse Data using Mouse Loggers. In Proceedings of the International Conference on Broadband and Wireless Computing, Communication and Applications, Asan, Korea, 5–7 November 2016

[3]Mellado, D.; Mouratidis, H.; Fernández-Medina, E. Secure Tropos Framework for Software Product Lines Requirements Engineering. Comput. Stand. Interfaces 2014, 36, 711–722

[4]Mohsin, M.; Anwar, Z.; Zaman, F.; Al-Shaer, E. IoTChecker: A data-driven framework for security analytics of Internet of Things configurations. Comput.Secur. 2017, 70, 199–223

[5]VeenooUpadhyay, SuryakantYadav Study of Cyber Security Challenges Its Emerging Trends: Current Technologies International Journal of Engineering Research and Management (IJERM) ISSN: 2349- 2058, Volume-05, Issue-07, July 2018

[6]Yim, K. A new noise mingling approach to protect the authentication password. In Proceedings of the 2010 International Conference on Complex, Intelligent and Software Intensive Systems, Seoul, Korea, 30 June–2 July 2012

[7]Nikita TresaCyriacLipsaSadath Is Cyber Security Enough- A study on Big Data Security Breaches in Financial Institutions 2019 4th International Conference on Information Systems and Computer Networks (ISCON) GLA University, Mathura, UP, India. Nov 21-22, 2019

[8]MdLiakat Ali Kutub Thakur Beatrice Atobatele Challenges of Cyber Security and the Emerging Trends BSCI'19, July 8, 2019, Auckland, New Zealand

[9]Kutub Thakur1, Meikang Qiu2∗, Keke Gai3, MdLiakat Ali4 An Investigation on Cyber Security Threats and Security Models 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing 978-1-4673-9300-3/15

[10] J. Li. The research and application of multi-firewall technology in enterprise network security. Int’l J. of Security and Its Applications, 9(5):153–162, 2015