IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 1, January 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 1, January 2021 ||

DOI:10.15680/IJIRSET.2021.1001041

Study of Cyber Security

Rohan Shinde[1], **Prof. Mrs. Rama S. Bansode**[2]

P. G. Student, Department Master of Computer Application, P.E.S. Modern College of Engineering, Pune, Maharashtra, India[1]

Research Scholar, TMV Pune Asst. Professor, P.E.S. Modern College of Engineering, Pune , Maharashtra, India[2]

ABSTRACT: Cybersecurity plays a crucial role in the field of data technology. Securing knowledge became one of the most important challenges within the present day. Whenever we expect about cybersecurity the primary thing that involves our mind is 'cybercrimes' which are increasing immensely day by day. Various Governments and corporations are taking many measures so as to stop these cybercrimes. Besides various measures, cybersecurity remains a really big concern to several. This paper mainly focuses on challenges faced by cybersecurity on the newest technologies. It also focuses on the latest about the cybersecurity techniques, ethics, and therefore the trends changing the face of cybersecurity.

I. INTRODUCTION

"Cybersecurity is primarily about people, processes, and technologies working together to encompass the entire range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including network operations, information assurance, enforcement, etc."
Cybersecurity is the protection of Internet-connected systems, including hardware, software, and data from cyber-attacks. It is made from two words one is cyber and the other is security. Cyber is claimed to the technology which contains systems, network and programs or data. Whereas security associated with protection which incorporates systems security, network security, and application, and knowledge security.
It is the body of technologies, processes, and practices designed to guard networks, devices, programs, and data from attack, theft, damage, modification, or unauthorized access. It may even be mentioned as information technology security.

II. WHAT IS CYBER SECURITY

Cybersecurity is all about reducing threats when people are in the process of dealing with technology. It encompasses the complete range of protection against any online risk or vulnerability, which comprises information security assurance and cyber enforcement. In other words, cybersecurity is that the protection of cyber-space (which includes hardware, software, networks, and their servers, peripheral devices, data and knowledge, and everyone other components related to technology) and internet-connected systems from both internal also as external threats and cybercriminals.
Cyber-attack is now a world concern and has given many concerns that hacks and other security attacks could endanger the worldwide economy. Organizations transmit sensitive data across networks and to other devices within the course of doing business, and cybersecurity describes to guard that information, and therefore the systems wont to process or store it.

III. TYPES OF CYBER SECURITY

1. Application Security: Application Security involves implementing various defenses within all software and services used within a corporation against a good range of threats. It requires designing secure application architectures, writing secure code, implementing strong data input validation, threat modeling, etc. to minimize the likelihood of any unauthorized access or modification of application resources.
2. Identity Management and Data Security: Identity management includes frameworks, processes, and activities that enables authentication and authorization of legitimate individuals to information systems within an organization. Data security involves implementing strong information storage mechanisms that ensure security of knowledge at rest and in transit.
3. Network Security: Network security involves implementing both hardware and software mechanisms to guard the

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 1, January 2021 ||

DOI:10.15680/IJIRSET.2021.1001041

network and infrastructure from unauthorized access, disruptions, and misuse. Effective network security helps protect organizational assets against multiple external and internal threats.

4. Mobile Security: Mobile security refers to protecting both organizational and personal information stored on mobile devices like cell phones, laptops, tablets, etc. from various threats like unauthorized access, device loss or theft, malware, etc.

5. Cloud Security: Cloud security relates to designing secure cloud architectures and applications for organization using various cloud service providers such as AWS, Google, Azure, Rack space, etc. Effective architecture and environment configuration ensures protection against various threats.

IV. CYBER CRIMES

Cybercrime is defined as either a criminal offense involving computing against a digital target or a criminal offense during which a computer system is employed to commit criminal offenses. As a broad category of crime, cybercrime includes such disparate kinds of activities as illegal access of knowledge, use of computer communications to commit fraud, or the ransoming of systems via digital means. Cybercrime can also be mentioned as computer crime.

The Information Technology Act 2000 or any legislation within the Country doesn't describe or mention the term Cyber Crime. It is often globally considered because of the gloomier face of technology. the sole difference between a standard crime and a cyber-crime is that the cyber-crime involves a crime associated with computers.

V. TYPES OF CYBER CRIME

1. Hacking: In simple words, hacking is an act committed by an intruder by accessing your computing system without your permission. Hackers (the people doing the 'hacking') are basically computer programmers, who have a complicated understanding of computers and commonly misuse this data for devious reasons.

2.Virus dissemination: Viruses are computer programs that attach themselves to or infect a system or files, and have a bent to circulate to other computers on a network. They disrupt the pc operation and affect the info stored – either by modifying it or by deleting it altogether. "Worms" unlike viruses don't need a number to cling on to. They merely replicate until they eat up all available memory within the system.

3. Logic bombs: A slag code, also referred to as "slag code", may be a malicious piece of code which is intentionally inserted into software to execute a malicious task when triggered by a specific event. It's not an epidemic, although it always behaves during a similar manner. It is stealthily inserted into the program where it lies dormant until specified conditions are met.

a.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 1, January 2021 ||

DOI:10.15680/IJIRSET.2021.1001041

VI. LAWS OF CYBER SECURITY

- **Information technology act, 2000**

The Indian cyber laws are governed by the knowledge technology act, penned down back in 2000. The principal impetus of this act is to supply reliable legal inclusiveness to ecommerce, facilitating registration of real-time records with the govt .

- **Indian penal code (ipc) 1980**

Identity thefts and associated cyber frauds are embodied within the Indian legal code (IPC), 1860 - invoked along side the knowledge technology act of 2000.

- **Companies act of 2013**

The corporate stakeholders ask the businesses act of 2013 because the legal obligation necessary for the refinement of daily operations. The directives of this act cements all the specified techno-legal compliances, putting the less compliant companies during a legal fix.

VII. BENEFITES OF CYBER SECURITY

Protect your business: The most important advantage is that the simplest IT security cyber security solution can provide comprehensive digital protection to your business. This will allow employees to surf the internet as and when they need, and ensure that they aren't at risk from potential threats.
Protects Personal Info: one of the foremost valuable commodities within the digital age is personal information. If an epidemic is in a position to get personal information regarding your employees or customers, they're quite capable of selling that information on, or maybe using it to steal their money.
Work Safety: Without the simplest cyber security solutions for your business, you and your employee are constantly in danger from a possible cyber-attack. If your system, or even individual computers, become infected then it will really hamper their productivity and even force you to exchange computers.

VIII.CONCLUSION

Today thanks to high internet penetration, cybersecurity is one of the most important needs of the planet as cybersecurity threats are very dangerous to the country's security. Not only the government but also the citizens should spread awareness among the people to always update your system and network security settings and to utilization proper anti-virus so that your system and network security settings stay virus and malware-free. All in all, small businesses are at a major risk of being hacked, there are methods that can help deter attackers from targeting business and looking elsewhere for softer targets to test their exploits. It's important to conduct a system-wide assessment to determine the current state of the business's security so as to know the next steps to take.

REFERENCES

[1] Redlich, R. M., &Nemzow, M. A. (2006). U.S. Patent No. 7,103,915. Washington, DC: U.S. Patent and Trademark Office.
[2] Chen, D., & Zhao, H. (2012, March). Data security and privacy protection issues in cloud computing. In 2012 International Conference on Computer Science and Electronics Engineering (Vol. 1, pp. 647-651). IEEE.
[3] Pfleeger, C. P., &Pfleeger, S. L. (2002). Security in computing. Prentice-Hall Professional Technical Reference.
[4] Witkowska, Wiktoria, Martina Ziefle, and Matt-MouleyBouamrane. "Privacy and Data Security in E-health: Requirements from the User's Perspective." Health Informatics Journal 18.3 (2012): 191-201. Web.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details