SURVEY ON CYBER SECURITY IN DIFFERENT SCENARIOS

[1]Dr.V.Vasanthi ,[2] J.Logeshwaran,[3]B.Vishnuvarthan

[1]Asst.Professor,PG& Research,Department Of Computer Applications
[2,3]II MCA, PG& Research,Department Of Computer Applications
Hindusthan College of Arts and Science Coimbatore,India.

Abstract:Cyber Security accepts a vigorous role in the area of information technology. Safeguarding the information has become an enormous problem in the current day. The cyber security the main thing that originates in mind is 'cyber crimes' which are aggregate colossally daily. Different governments and organizations are taking numerous measures to keep these cyber wrongdoings. Other than different measures cyber security is as yet a significant worry to many. This paper mostly emphases on cyber security and cyber terrorism. The significant trends of cyber security and the consequence of cyber security discuss in it. The cyber-terrorism could make associations lose billions of dollars in the region of organizations. The paper also explains the components of cyber terrorism and motivation of it. Two case studies related to cyber security also provide in this paper. Some solution about cyber security and cyber terrorism also explain in it.

Keywords: cybersecurity survey, security survey, trends cybersecurity, cybersecurity network

I. INTRODUCTION

Today an individual can receive and send any information may be video, or an email or only through the click of a button but did s/he ever ponder how safe this information transmitted to another individual strongly with no spillage of data? The proper response lies in cybersecurity. Today more than 61% of full industry exchanges are done on the internet, so this area prerequisite high quality of security for direct and best exchanges. Thus, cybersecurity has become a most recent issue (Dervojeda, et. all., 2014). The extent of cybersecurity does not merely restrict to verifying the data in IT industry yet also to different fields like cyberspace and so forth. Improving cybersecurity and ensuring that necessary data systems are vital to each country's security and financial prosperity.

1.1.PURPOSE

The paper provides information about cyber security and cyber terrorism. It covers various information about these topics in its subsections. Trends of cybersecurity and the role of social media in cybersecurity define in this paper. The paper provides some necessary information about cyber terrorism. The components of "cyber terrorism" and the consequences of this terrorism also explain in this paper. There are some examples of case studies those related to cybersecurity. The paper also provides some solutions regarding cyber security and cyber terrorism. It provides some techniques for preventing cyber terrorism. The future study and scope of cybersecurity define in it. Cybersecurity has become a major concern over the last 10 year in the IT world. In the present world, everybody is facing a lot of problems with cybercrime. As hackers are hacking major sensitive information from government and some enterprise organizations the individuals are very much worried as cybersecurity assault can bring about everything from wholesale fraud, to blackmail big companies. They are many varieties of cyber-crimes emerging where everyone needs to be aware of the scams and they are different measures and tools which can be used for avoiding the cyber-crimes. Every organization wants to secure their confidential data from getting hacked. Getting hacked is not just about losing the confidential data but losing the relationship with customers in the market (Bendovschi, 2015)

2. TRENDS OF CYBER SECURITY

Cyber Security assumes a critical role in the area of data technology. Safeguarding the data have become the greatest difficulty in the current day. The cybersecurity the main thing that raids a chord is cybercrimes which are increasing tremendously step by step (Samuel, & Osman, 2014). Different administrations and organizations are taking many measures to keep these cybercrimes. Additional the different measures cyber security is as yet an enormous worry to numerous. Some main trends that are changing cyber security give as follows.

2.1 Web servers

The risk of assaults on web applications to separate information or to circulate malicious code perseveres. Cybercriminals convey their code using good web servers they have traded off. In any case, information taking attacks, a considerable lot of which get the deliberation of media, are also a significant risk. Currently, individuals need a more unusual accentuation on securing web servers as well as web applications (Bendovschi, 2015). Web servers are mainly the preeminent stage for these cybercriminals to take the information. Thus, one should reliably utilize an additional secure program, mainly amid vital exchanges all together not to fall as a quarry for these defilements.

2.2 Mobile Networks

The risk of assaults on web applications to separate information or to circulate malicious code perseveres. Cybercriminals convey their code using good web servers they have traded off. In any case, information taking attacks, a considerable lot of which get the deliberation of media, are also a significant risk. Currently, individuals need a more unusual accentuation on securing web servers as well as web applications (Bendovschi, 2015). Web servers are mainly the preeminent stage for these cybercriminals to take the information. Thus, one should reliably utilize an additional secure program, mainly amid vital exchanges all together not to fall as a quarry for these defilements.

2.3 Encryption

It is the method toward encoding messages so programmers cannot scrutinize it. In encryption, the message is encoded by encryption, changing it into a stirred-up figure content. It commonly completes with the use of an “encryption key,” that demonstrates how the message is to encode. Encryption at the earliest reference point level secures information protection and its respectability (Sharma, 2012). Additional use of encryption obtains more problems in cybersecurity. Encryption is used to ensure the information in travel, for instance, the information being exchanged using systems (for example the Internet, online business), mobile phones, wireless radios and so on.

2.4 ADP’s and targeted attacks

Advanced Persistent Threat (APT) is a whole of the dimension of cybercrime ware. For quite a long time network security capacities. For example, IPS or web filtering have had a key influence in distinguishing such focused-on assaults (Bendovschi, 2015). As attackers become bolder and utilize increasingly dubious methods, network security must incorporate with other security benefits to identify assaults. Thus, one must recover our security procedures to counteract more dangers coming later on. Subsequently the above is a portion of the patterns 118 Unauthentifiziert | Heruntergeladen changing the essence of cybersecurity on the planet.

3. ROLE OF SOCIAL MEDIA IN CYBER SECURITY

Social media has turned into a lifestyle for some individuals. We use it to stay in contact, plan occasions, share our photographs and comment on recent developments. It has replaced email and telephone requires a ton of us. However, similarly as with whatever else on the web, it is imperative to know about the dangers. PCs, cell phones, and different gadgets are priceless assets that furnish people of any age with the extraordinary capacity to connect and collaborate with whatever remains of the world. Individuals can do this in various ways, including the utilization of social media or networking sites. Courtesy of social media, people can share musings, pictures, exercises, or any part of their lives (Gross, Canetti & Vashdi, 2017). They can bring an unknown look into the lives of others, regardless of whether they live nearby or over the globe. Unfortunately, these networks additionally represent security toward one's PC, protection, and even their security. Social media collection among faculty is soaring as is the risk of assault (Sharma, 2012). Since social media sites are nearly utilized by the majority of them reliably, it has become an excellent stage for cybercriminals for hacking private data and taking significant data.

3.1 CYBER TERRORISM

Social media has turned into a lifestyle for some individuals. We use it to stay in contact, plan occasions, share our photographs and comment on recent developments. It has replaced email and telephone requires a ton of us. However, similarly as with whatever else on the web, it is imperative to know about the dangers. PCs, cell phones, and different gadgets are priceless assets that furnish people of any age with the extraordinary capacity to connect and collaborate with whatever remains of the world. Individuals can do this in various ways, including the utilization of social media or networking sites. Courtesy of social media, people can share musings, pictures, exercises, or any part of their lives (Gross, Canetti & Vashdi, 2017). They can bring an unknown look into the lives of others, regardless of whether they live nearby or over the globe. Unfortunately, these networks additionally represent security toward one's PC, protection, and even their security. Social media collection among faculty is soaring as is the risk of assault (Sharma, 2012). Since social media sites are nearly utilized by the majority of them reliably, it has become an excellent stage for cybercriminals for hacking private data and taking significant data.

3.2 CYBER TERRORISM

The term “terrorism” can allude to the illegal utilization of power or viciousness against people in order to threaten an administration or its residents and associations which might be to accomplish a political or a malicious site [10]. Terrorism has transformed from the conventional structure to the cyber type of innovation supported terrorism recognized as cyber terrorism. It stays vital issues of the present society. Not just that the battle against terrorism is falling behind, current cybercrime assaults are ending up progressively forceful and confrontational (Sharma, 2012). This terrorism is the utilization of cyber word to dispatch an assault to the essential foundations that the presence of associations and countries entirely depended after that can prompt its shut down.

3.3 SOLUTIONS

Some solutions regarding cyber security and cyber terrorism describe here:

• Cyber Security Techniques Some techniques can use to improve cybersecurity.

• Access control and “password security”: The idea of password and user name has a primary method for ensuring data. It may be the principal measures concerning cybersecurity.

• Data’s Authentication: The documents that we get should dependably be validated be before transferring. It should check if it has begun from a critical and dependable source and that they are not modified (Gade, & Reddy, 2014). Verifying of these records is typically done by the “antivirus” software present in the gadgets. Subsequently, a decent “antivirus” software is likewise necessary to shield the gadgets from viruses.

• Anti-virus software: It is a PC program that classifies, avoids, and makes a move to harm or evacuate noxious software programs, for instance, viruses as well as worms. Most "antivirus programs" comprise an "autoupdate" feature that authorizes the program to download profiles of new viruses with the objective that it can chequer for the new viruses when they find.

• Malware scanners: This is software that typically filters each of the records and archives current in the framework for vindictive code or destructive viruses [10]. Viruses, worms, as well as Trojan horses, are instances of “malicious software” that regularly assemble and alluded to as malware.

• Firewall: A “software program” or an equipment that helps monitor hackers, infections, and all types of worms which endeavour to achieve PC over the Internet. All data which is transmitting to and fro over the web go through the firewall contemporary, which looks at every.

4.PREVENTION OF CYBER TERRORISM

The capacity to prevent cyber terrorism lies with the capacity to securely verify cyberspace. Cybersecurity has an intriguing parallel to terrorism. Both are lopsided. Guaranteeing the security of information, data, and correspondence is impressively harder than hacking into a framework. The attacker has an inalienable preferred standpoint in both regular terrorism and cyber-attacks. On account of state-supported attacks, the difficulties are of a lot higher greatness (Cabaj, Kotulski, Księżopolski, & Mazurczyk, 2018). Governments should guarantee that their rules smear to cybercrimes and be wholly actualized and hold fast to; it is essential that the countries of the biosphere take measures to guarantee that its punitive and technical law is satisfactory to address the difficulties presented by cybercrimes (Kumar, & Somani, 2018). The availability, confidentiality and the integrity of information in any associations are essential which endeavors must be set up to guarantee that they are exceptionally secure because it is the significant cyber resource that makes each association stand and in the meantime depended upon. The information has entered by the “cyber-terrorist” is something beyond records which may incorporate messages, web applications, web pages, and just as some indispensable operating systems. (Kumar, & Somani, 2018).

5. CONCLUSION

Cyber-security is both about the insecurity made by and through this new space and about the practices or procedures to make it (progressively) secure. Exertion to verify the cyberspace should give a definitive need else the "information technology" will not be viably used by clients. The terrorist of things to come will win the wars without discharging a shot just by crushing the country's necessary substructure if steps are not taken to handle the pervasiveness of the expansion in such a cyber-attack. They can bring an unknown look into the lives of others, regardless of whether they live nearby or over the globe. The “cyber-terrorism” can in one method or alternate prompts the death toll just as causing severe harms. Though social media can utilize for cybercrimes, these organizations cannot stand to quit utilizing social media as it assumes an essential role in the attention of an organization. Cyber terrorism has guaranteed numerous innocent lives and in the meantime render numerous homes to a condition of the problem that is occasionally coming about to mental injury to the influenced families. Cyber terrorism stays vital issues of the present society. Not just that the battle against Cyber terrorism is falling behind, current cybercrime assaults are ending up progressively forceful and confrontational. Cybersecurity has an intriguing parallel to terrorism. Guaranteeing the security of information, data, and correspondence is impressively harder than hacking into a system.

6. FUTURE STUDY AND SCOPE

This paper will help to advance the scientific interests in the exploration of cybersecurity, particularly to respond to the procedural questions of the prediction of future data and actions significant to security patterns. This study sets the background to begin executing rules for all intentions as indicated through the usual security issues and answers for data systems. This paper consolidates many procedures connected and may be improved to serve cybersecurity regarding anticipating the operational legitimacy of the methodologies of assessment benchmarks. Finally, the emphasis on limiting, recouping, and disposing of weakness is the primary, basic patterns, and reactions to the constant expanding progress (Panchanatham, 2015).

7. References

1. Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. Procedia Economics and Finance, 24-31. doi:10.1016/S2212-5671(15)01077-
2. Cabaj, K., Kotulski, Z., Księżopolski, B., & Mazurczyk, W. (2018). Cybersecurity: trends, issues, and challenges. EURASIP Journal on Information Security. doi:10.1186/s13635- 018-0080-0
3. Dervojeda, K., Verzijl, D., Nagtegaal, F., Lengton, M., & Rouwmaat, E. (2014). Innovative Business Models: Supply chain finance. Netherlands: Business Innovation Observatory; European Union.
4. Gade, N. R., & Reddy, U. G. (2014). A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies. Retrieved from https://www.researchgate.net/publication/260126665_A_Study_Of_Cyber_Security_Challenges_And_Its_Emerging_Trends_On_Latest_Technologies
5. Gross, M. L., Canetti, D., & Vashdi, D. R. (2017). Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes. Journal of Cybersecurity, 3(1), 49–58. doi:10.1093/cybsec/tyw018
6. Hua, J., & Bapna, S. (2013). The economic impact of cyber terrorism. The Journal of Strategic Information Systems, 22(2), pp. 175-186.
7. Kumar, S., & Somani, V. (2018). Social Media Security Risks, Cyber Threats And Risks Prevention And Mitigation Techniques. International Journal of Advance Research in Computer Science and Management, 4(4), pp. 125-129.
8. Panchanatham, D. N. (2015). A case study on Cyber Security in E-Governance. International Research Journal of Engineering and Technology.
9. Samuel, K. O., & Osman, W. R. (2014). Cyber Terrorism Attack of The Contemporary Information Technology Age: Issues, Consequences and Panacea. International Journal of Computer Science and Mobile Computing, 3(5), pp. 1082-1090.
10. Sharma, R. (2012). Study of Latest Emerging Trends on Cyber Security and its challenges to Society. International Journal of Scientific & Engineering Research, 3(6).
11. Sreenu, M., & Krishna, D. V. (2017). A General Study on Cyber-Attacks on Social Networks. IOSR Journal of Computer Engineering (IOSR-JCE), 19(5), pp. 01-04.
12. Sutton, D. (2017). Cyber Security : A Practitioner’s Guide. Swindon, UK: BCS, the Chartered Institute for IT.