International Journal of Applied Research 2019; 5(6): 439-441

ISSN Print: 2394-7500
ISSN Online: 2394-5869
Impact Factor: 5.2
IJAR 2019; 5(6): 439-441
www.allresearchjournal.com
Received: 27-04-2019
Accepted: 30-05-2019

Sandeepi
Assistant Professor, Department of Computer Science, Govt. P.G. College, Safidon, Haryana, India

Corresponding Author:
Sandeepi
Assistant Professor, Department of Computer Science, Govt. P.G. College, Safidon, Haryana, India

Cyber security: Challenges and emerging trends

Sandeepi

Abstract
There is no doubt in denying the fact that in the field of information technology cyber security is playing a significant and vital role as to secure the information is the need of the hour that is threatening now and again in the contemporary world. In that sense, it has become the biggest challenge in the present time. The idea of cyber crime comes in to our mind at once when we come across the about the cyber security. Many protective measures are being taken by various governments and companies, and the main reason behind it is how to prevent cyber crimes. But, in spite of many protective measures taken by various organizations, the problem of cyber security is a grim issue. In the present paper, an attempt has been made to focus on different challenging faced by cyber security on the latest technologies. This paper also throws light on some latest cyber security techniques, trends, ethics and challenges faced by the contemporary world.

Keywords: Technology, information, trends, security, leakage

Introduction
Nowadays to receive message and to send the messages is quite easy for men through e-mails or an audio or video just by clicking a button, but the question is whether man has ever taken into consideration the safety and security of these messages. In other words, whether man is conscious about the safety of the information without any leakage, the answer to this question lies in the concept of cyber security. Without any shadow of doubt, internet today is considered as the fastest and growing mean in everyday life. In the present scenario, the face of mankind is being changed due to some emerging technologies, but at the same time, we are unable to safeguard our private information in a very effective way and consequently, these days the cyber crimes are growing day by day.

No doubt, more than 60 percent of total transactions are on line today due to which the cyber security has become the latest issue. But, the scope of cyber security is not merely confined related to secure the information in IT industry, but its scope is extended to various other fields like cyber space. Even in present scenario, the latest technologies like cloud computing, mobile computing, net banking, and E-commerce are also to be taken into account from security point of view. There is no doubt that these technologies hold some information regarding a person their security has become the need of the hour. To increase cyber security and protecting critical information infrastructure is the key factor to each nation's security and economic well-being. Making the internet safer has become the central concern as it is an integral factor to the development of new services as well as governmental policy. Today, there is an utmost need of those aspects as the fight against cyber crime needs a comprehensive and safer approach.

It is an established fact that only technical measures are not sufficient to prevent any crime, in that situation, the law imposed by some agencies are required to investigate and prosecute cyber crime effectively. At present, many nations and governments are imposing strict laws in this issue of cyber securities so that the loss of some vital information can be stopped. So, it becomes important for each individual to take some protective measures to save themselves from growing cyber crimes. Now the question arises regarding the term what is cyber crime? It is a term devised for any illegal activity that uses a computer for its primary means of communication and theft.

According to U.S. department of justice which expands the same term by defining cyber crime to include any illegal activity that uses a computer for the storage of evidences. Among the growing list of cyber crimes can be include crimes made possible by the computers.

Among these crimes the network intrusions and dissemination of computer viruses, computer based variation of existing crimes like identity theft, stalking bullying and terrorism are worthy of detailed considerations. These are, no doubt, among the major problems of people and nations as well. In general sense, cyber crime may be explained as crime committed using a computer and the internet steel a person's identity or sell contraband or stalk victims or disrupt operations with malevolent programs. With the passage of time, technology is playing an important role in man's life which further, will enhance the cyber crimes in future.

Any organization would like to take care of two factors namely privacy and security which are considered as the top security measures. At present, we are living in a world where all the information is maintained in a digital or a cyber form. Social networking sites provide a space where users feel safe as they interact with friends and family. As far as the home users are concerned, cyber-criminals would continue to target social media sites to steal personal data. Not only social networking, but also during bank transactions a person must take all the required security measures.

Trends changing cyber security

Here are recommended some of the trends that affect, to a large extent, cyber security.

1. **Web servers:** The threat of attacks on web applications to extract data or to distribute malicious code persists. Cyber criminals distribute their malicious code via legitimate web servers they've compromised. But data-stealing attacks, many of which get the attention of media, are also a big threat. Now, we need a greater emphasis on protecting web servers and web applications. Web servers are especially the best platform for these cyber criminals to steal the data. Hence one must always use a safer browser especially during important transactions in order not to fall as a prey for these crimes.
2. **Cloud computing and its services:** These days all small, medium and large companies are slowly adopting cloud services. In other words the world is slowly moving towards the clouds. This latest trend presents a big challenge for cyber security, as traffic can go around traditional points of inspection. Additionally, as the number of applications available in the cloud grows, policy controls for web applications and cloud services will also need to evolve in order to prevent the loss of valuable information. Though cloud services are developing their own models still a lot of issues are being brought up about their security. Cloud may provide immense opportunities but it should always be noted that as the cloud evolves so as its security concerns increase.
3. **APT's and targeted attacks:** APT (Advanced Persistent Threat) is a whole new level of cyber crime ware. For years network security capabilities such as web filtering or IPS have played a key part in identifying such targeted attacks (mostly after the initial compromise). As attackers grow bolder and employ more vague techniques, network security must integrate with other security services in order to detect attacks. Hence one must improve our security techniques in order to prevent more threats coming in the future.
4. **Mobile Networks:** Today we are able to connect to anyone in any part of the world. But for these mobile networks security is a very big concern. These days, firewalls and other security measures are becoming porous as people are using devices such as tablets, phones, PC's etc all of which again require extra securities apart from those present in the applications used. We must always think about the security issues of these mobile networks. Further mobile networks are highly prone to these cyber crimes a lot of care must be taken in case of their security issues.
5. **IPv6:** New internet protocol IPv6 is the new Internet protocol which is replacing IPv4 (the older version), which has been a backbone of our networks in general and the Internet at large. Protecting IPv6 is not just a question of porting IPv4 capabilities. While IPv6 is a wholesale replacement in making more IP addresses available, there are some very fundamental changes to the protocol which need to be considered in security policy. Hence it is always better to switch to IPv6 as soon as possible in order to reduce the risks regarding cyber crime. 4.6 Encryption of the code Encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it. In an encryption scheme, the message or information is encrypted using an encryption algorithm, turning it into an unreadable cipher text. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Encryption at a very beginning level protects data privacy and its integrity. But more use of encryption brings more challenges in cyber security. Encryption is also used to protect data in transit, for example data being transferred via networks (e.g. the Internet, ecommerce), mobile telephones, wireless microphones, wireless intercoms etc. Hence, by encrypting the code one can know if there is any leakage of information. Hence, the above are some of the trends changing the face of cyber security in the world.

Conclusion

it goes without saying that the concept of security regarding information in the present time is a burning issue that is gaining momentum with time. At the same time, is a significant issue as in the age of globalization all the countries are coming together and are getting interconnected as with the network being used to carry out critical transaction. It has been witnessed that cyber crime continues to diverge down different paths every year that passes and same happens to the security of information. The latest and most suitable technology, along with the new cyber tools and threats that come to light each day, are challenging different organizations time and again with not only how they secure their infrastructure, but how they are searching for new platforms and other tactics to in order to overcome this serious problem. As it is clearly evident that there is no perfect solution for this grim problem but the thing is that we should try to minimize them so that to have a safe and secure future in cyber space.

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 Net Action Report by Audrie Krause.
4. A Look back on Cyber Security by Luis Corrons - Panda Labs, 2012.
5. International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September Page nos. 68 - 71 ISSN 2229-5518, Study of Cloud Computing in Health Care Industry by G. Nikhita Reddy, G.J. Ugander Reddy, 2013.
6. IEEE Security and Privacy Magazine - IEEECS Safety Critical Systems - Next Generation July/ Aug 2013. 7. CIO Asia, September 3rd, H1 Cyber security in Malasia by Avanthi Kumar, 2013.
7. Yang Miao. ACM International Conference Proceeding Series, vol. 113.
8. Unisys Corporation, Unisys Descriptive Technology & Trends Points of White Paper Series- Cyber Security USA, 2011.
9. Cyber Security Strategy of United Kingdom, 2009.
10. ITU Cyber Security Work Program to Assist Development Countries, 2009, (6) Rev. Jonames Burg, TTU WTSA Resolution 50, 2008.
11. ITU Cyber Security Work Program to Assist Development Countries, 2008.
12. Kellermann, Technology Risk Checklist, Cybercrime and Security, IIB-2.
13. Schjolberg/Hubbard, Harmonizing National Legal Approaches on Cybercrime, 2005.
14. The most Important Instruments in fight against Cybercrime, Ch. 6.2.
15. Luis Corrons, Technical Director, Panda Labs, Bangalore, 2012.