International Journal of Research in Engineering
www.engineeringpaper.net
Online ISSN: 2664-8784; Print ISSN: 2664-8776
Received: 15-04-2020; Accepted: 05-05-2020; Published: 08-06-2020
Volume 2; Issue 1; 2020; Page No. 22-24

A comprehensive study on need of cyber security

Justin Devassy[1], Abhishek Bharadwaj[2], Dr. Deepak Chahal[3]
[1-3] Department of IT, Jagan Institute of Management Studies, Sector -05, Rohini, New Delhi

DOI: https://doi.org/10.33545/26648776.2020.v2.i1a.29

Abstract
Cyber Security plays a huge role in the current field of information technology. With security of the information becoming one of the biggest problems in the world. When we think about the cyber security the first thought that comes to our mind is ‘cyber crimes’ which are greatly rising day by day. Various Private companies and Governments are taking necessary actions to stop these cyber-crimes. Besides various measures cyber-crimes are still a big concern for everyone. This paper’s main motive is to show various challenges faced by cyber security around the world and most used technologies. It also sheds light on latest cyber security techniques, ethics, measures and the trends of cyber security.

Keywords: security, technology, application

Introduction

Cyber security is the practice of defending of Networks, Server, Databases, Mobile devices, Electronic systems, and data from malicious attacks. The objective of cyber security is to establish rules and measure to use against attacks over the internet. Cybercrime can be categorize in three different aspects one is the computer as a target in which attacker or hacker uses a computer to attacks other computer using Virus, Worms, Phishing, Spyware, Ransomware, Adware, Botnets DoS attack etc and second one is computer as a weapon in which computer are used to commit real world crime e.g. credit card fraud, identity theft etc. And the third one is Cyber terrorism is intended to undermine electronic systems to cause panic or fear. Cyber security is made up of two words first cyber related to the technology which contains systems, network and programs or data and other is security related to the protection which includes systems security, network security and application and information security. Other word for cyber security is information technology security or electronic information security. A focus is made on machines as machines cannot be understood by verbal communication it forms abstractions and concepts [1].

Need of Secure Web Application

There should be the mechanism to Protect websites and online services against different security risks that exploit vulnerabilities in an application’s code as attacker can manipulate sensitive private data collected which are often exploited to either manipulate source code or gain unauthorized access. Common targets for web application attacks are content management systems such as WordPress and database administration tools like phpMyAdmin. Some Web Applications vulnerabilities such as SQL Injection(malicious SQL code to manipulate a backend database so it reveals information), Cross-site Scripting (XSS injection attack targeting users in order to access accounts, activate Trojans or modify page content), Remote File Inclusion (attack to remotely inject a file onto a web application server) and Cross-site Request Forgery (CSRF attack that could result in an unsolicited transfer of funds, changed passwords or data theft). It is a responsibility of website administrator ensures safety of web application in order to prevent unauthorized access and data theft. Security is looked in terms of how data is stored, coded, transmitted, encrypted and deleted. Various statistics has shown that companies take security of the data of an individual with very high priority [2].

Securing Web Application

- Error Handling and logging: Website administrator or developer should handle all exceptions, suppress all framework generated errors, should log all authentication and validation attempts, admin activities, all privilege changes, access to sensitive files and data store and maintain backup of all logs.
- Configuration and operations: System Administrator should configure and define all security requirements perform design revises, code reviews, security testing. Performing risk analysis and strategize an incident handling plans.
- Authentication: A user should not use default credentials, should use strong password and change password frequently and website administrator should use strong password policy and give minimal privileges to middleware. Soring credentials in salted hashes in databases. Setting up Two factor authentication which uses OTP (one-time password) to authenticate user.
- Session Management: Web application should be developed in such a way that create random session tokens, regenerate token after any changes made, implementation of session timeouts. Using secure cookies, setting up of cookie expirations and implementation of concurrent session carefully so that it may not hamper any user activity.
- Input and Output handling: Every input or output of data or request should be handled every carefully as most of the time attacker stole vital information in these requests of web applications. Implementing input/output encoding, using

HTML encoding, validating file uploads (type, extension, MIME etc.).

- Bounty program Control: Bounty program Control is a great way to get feedback from the community regarding web application security. This encourage the community to find security risks and report them in return a bounty is offered in monetary value as a reward to the user. Bounty program are used to help reduce the risk of any security issues and provide users the chance to be rewarded and get fame in community.

Challenges

Cyber-attacks are very alarming in financial sector as the amount of cyber-crimes in financial sector are the most when compared to any other sector. The amount of cybercrime is substantial in financial sector which leads to huge role in reputation of banks. Financial sectors like banking sector are more likely to be targeted compared to any other financial sector.

Cyber-security measures of banking sectors which for the ease of the user makes web-based services like websites and mobile applications which are easy to target if the security is low either end of user or bank. Many cybercriminals target online and mobile banking system using multiple tricks even malwares. Cyber attackers hack customer or employees' details and hack the security system of the bank.

Let's look at the various cyber security threat facing the banking sector

Identity theft

Every year it is estimated that the banking sector suffers a loss of millions through identity theft. Research says, over 10 lakh Customer in India have faced Identity theft in past 4 years. This leads to use of person's identity and card information without their knowledge for purchasing and debiting of money.

Threat from employees

Multiple breaches in financial sector are because of human error. These errors are usually caused by employees such as employee leaking information related to security to hacker for money or because of extortion of some personal data. Some cases include where employees access their emails and click some phishing links which download some malware which may end up infecting the whole system and jeopardize the security. For such situations to not occur cyber security training is given to employees. In some countries, secrecy rules prevent banks from revealing financial information about their customers to foreign regulators [3].

Ransomware

One of the biggest hit to the baking sector which lead to a huge turmoil for people in service sector. Ransomware is a software threat that confined the service of the victim until the ransom money is paid to the hacker. Individuals are prone to this attack when they open a link in a suspicious email which leads to a malicious software into computer usually carried out in Trojan file disguised as a legitimate file.

UPI scams

Some of the most recent scams in India is where people who want to receive payments are given a link by buyers. These links actually makes you send money to the buyer, some people are gullible and end up being victim of such simple scams.

Fake Bank Scams

These scams usually happen through calls where people impersonating as bank employees tell you that your debit card is going to cancel and ask for personal details such card number, CVV, security questions etc. People need to be more aware of such scams individuals should know how private is their banking data.

Challenges in social media

Social Media has come with its own sets of scams and other cybercrimes from murders to Kidnapping and even terror attacks have been plotted using social media.

Misusing Identity

The attacker impersonates identity of any user results in misusing identity. The attacker may end making demands with people who are friends of the victim some of most common cases are asking for money. Defamation by posting obscene content. Misuse of identity has also lead to death and kidnapping of individuals

Threats From Using 3rd Party Applications

These applications seek permission from the user to access personal information for various applications including camera, storage, microphone etc. The user grants the app a certain level of permission leading too mining of personal details and passwords. And some of these applications which are working at background may download a malware on the user's computer or phone without their knowledge.

Viruses, Phishing and Malwares

Viruses and malware often end up into computer by clicking at advertisements. After gaining access to the computer and network, the attacker can steal individual's data and may end up infecting others by sending same spam email using the victim's network and mails.

Legal Issues

Posting contents that is offensive to any individual or community or religion. There legal terms and conditions associated with social networking sites like leaking confidential information on sites or posting child pornography or cyber bullying.

Conclusion

As we have seen above why cybersecurity plays a crucial role in our day to day lifestyle. As we have learned about various cybersecurity attacks like Identity theft, Ransomware, Threat from employees, UPI scams, Fake Bank Scams, Misusing Identity, Threats From Using 3rd Party Applications, Viruses, Phishing, Malware, Legal Issues are some of the Cyber attacks which are conducted in all over the world. The rate of conducting cybercrime is increasing every year. Now, these days we all access internet but most of us still don't know how to stay safe on the internet or any other scams which are active. Cybersecurity statics shows that 52% of breaches were related to hacking, 28% were related to malware and 32% were related to phishing. Social media platforms and other messaging platforms emerging as a new ground for criminal deception. Government and various big IT firms are investing billions of dollar to protect their firms from such attacks. In order to protect our self and other we should start with basics of how to stay safe and keep informed of all the new fundamental activities which are in trend. Reporting the cybercrime is also a good step to letting inform Government agencies which can track down these fraudsters down and take action accordingly.

References

1. Kharb L, *et al*. “Brain Emulation Machine Model for Communication” in International Journal of Scientific & Technology Research (IJSTR), 2019, 1410-1418.
2. Bhutani S, *et al*, Data privacy and security issues in India: An empirical study, International Journal of Research in Engineering. 2019; 1(4):15-17.
3. Chahal D, *et al*. Blockchain: An Innovative Technology, International Journal of Scientific Research and Engineering Development, 2019, 2(6).