A STUDY OF CYBER SECURITY CHALLENGES AND ITS EMERGING TRENDS ON LATEST TECHNOLOGIES

Dhiraj Yuvraj Bhosale

Student, M.Sc IT, Keraleeya Samajam (Regd.) Dombivli's Model College, Maharashtra, India

---***---

Abstract – Cyber Security plays a vital role within the field of data technology .Securing the data have become one amongst the most important challenges within the gift day. once ever we expect concerning the cyber security the primary issue that involves our mind is 'cyber crimes' that area unit increasing vastly day by day. numerous Governments and firms area unit taking several measures so as to forestall these cyber crimes. Besides numerous measures cyber security remains a awfully massive concern to several. This paper principally focuses on challenges two-faced by cyber security on the newest technologies .It additionally focuses on latest concerning the cyber security techniques, ethics and therefore the trends ever-changing the face of cyber security. Cyber Security plays a crucial role within the field of knowledge technology. This paper primarily focuses on challenges visaged by cyber security on the most recent technologies. It additionally focuses on latest concerning the cyber security techniques, ethics and also the trends dynamic the face of cyber security. Securing the data became one amongst the largest challenges within the gift day. Whenever we expect concerning the cyber security the primary factor that involves our mind is 'cyber crimes' that area unit increasing vastly day by day. numerous Governments and firms area unit taking several measures so as to forestall these cybercrimes. Besides numerous measures cyber security continues to be a awfully huge concern to several. numerous Governments and firms area unit taking several measures so as to forestall these cyber crimes. Besides numerous measures cyber security remains a awfully massive concern to several. This paper principally focuses on challenges two-faced by cyber security on the newest technologies .It additionally focuses on latest concerning the cyber security techniques, ethics and therefore the trends ever-changing the face of cyber security.

Key Words: cyber security, cyber crime, cyber ethics, social media, cloud computing, android apps.

1. INTRODUCTION:

Today man is ready to send and receive any type of data is also associate degree e-mail or associate degree audio or video just by the clicking of a howeverton but did he ever think however firmly his knowledge id being transmitted or sent to the opposite person safely with none leakage of information?? the solution lies in cyber security. nowadays net is that the quickest growing infrastructure in a day life. In today's technical atmosphere several latest technologies area unit ever-changing the face of the person kind. however because of these rising technologies we area unit unable to safeguard our non-public information terribly} very effective manner and thus these days cyber crimes area unit increasing day by day. nowadays quite sixty % of total commercial transactions area unit done on-line, so this field needed a top quality of security for transparent and best transactions. thus cyber security has become a contemporary issue. The scope of cyber security isn't simply restricted to securing the information in IT trade however additionally to numerous other fields like cyber house etc.

Even the newest technologies like cloud computing, mobile computing, E-commerce, net banking etc additionally wants high level of security. Since these technologies hold some necessary information concerning an individual their security has become a requirement factor. Enhancing cyber security and protective crucial data infrastructures area unit essential to every nation's security and economic eudaimonia. Making the Internet safer (and protective net users) has become integral to the event of latest services also as governmental policy. The fight against cyber crime wants a comprehensive and a safer approach. Given that technical measures alone cannot stop any crime, it's crucial that enforcement agencies area unit allowed to analyze and prosecute cyber crime effectively. Today many nations and governments area unit imposing strict laws on cyber securities so as to stop the loss of some necessary data. Every individual should even be trained on this cyber security and save themselves from these increasing cyber crimes.

2. CYBER CRIME

Cyber crime may be a term for any criminal activity that uses a pc as its primary means that of commission and felony. The U.S. Department of Justice expands the definition of cyber crime to include any criminal activity that uses a pc for the storage of proof. The growing list of cyber crimes includes crimes that are made attainable by computers, like network intrusions and also the dissemination of pc viruses, also as computer-based variations of existing crimes, like identity theft, stalking, bullying and coercion that have become as major drawback to folks and nations. typically in common man's language cyber crime is also outlined as crime committed using a pc and also the net to steel a person's identity or sell contraband or stalk victims or disrupt operations with malevolent. Cybercrime is criminal activity that either targets or uses a laptop, a electronic network or a networked device. Most, however not all, law-breaking is committed by cybercriminals or hackers WHO wish to form cash. law-breaking is allotted by people or organizations.

Some cybercriminals area unit organized, use advanced techniques and area unit extremely technically mean. Others area unit novice hackers. Rarely, law-breaking aims to break computers for reasons aside from profit. These may be political or personal. Cybercrime that stops users employing a machine or network, or prevents a business providing a code service to its customers, is termed a Denial-of-Service (DoS) attack. Cybercrime that uses computers to commit alternative crimes might involve exploitation computers or networks to unfold malware, contraband data or contraband pictures. Sometimes cybercriminals conduct each classes of law-breaking promptly. they will target computers with viruses 1st. Then, use them to unfold malware to alternative machines or throughout a network. Cybercriminals can also perform what's called a Distributed-Denial-of-Service (DDos) attack. this can be almost like a DoS attack however cybercriminals use various compromised computers to hold it out. The North American nation Department of Justice acknowledges a 3rd class of law-breaking that is wherever a laptop is employed as an adjunct to crime. associate example of this can be employing a laptop to store taken knowledge.

The North American nation has signed the ecu Convention of law-breaking. The convention casts a good internet and there area unit various malicious computer-related crimes that it considers law-breaking.

3. CYBER SECURITY

Privacy and security of the info can invariably be top security measures that any organization takes care. we tend to ar presently living during a world where all the knowledge is maintained during a digital or a cyber kind. Social networking sites provide an area wherever users feel safe as they interact with friends and family. within the case of

home users, cyber-criminals would still target social media sites to steal personal information. Not solely social networking however additionally throughout bank transactions someone should take all the specified security measures. Cyber security is that the observe of defensive computers, servers, mobile devices, electronic systems, networks, and information from malicious attacks. it is also referred to as data technology security or electronic data security. The term applies during a style of contexts, from business to mobile computing, and might be divided into many common classes. Network security is that the observe of securing a electronic network from intruders, whether or not targeted attackers or opportunist malware. Application security focuses on keeping package and devices freed from threats. A compromised application might offer access to the info its designed to shield. winning security begins within the style stage, well before a program or device is deployed.

Information security protects the integrity and privacy of knowledge, each in storage and in transit. Operational security includes the processes and selections for handling and protective information assets. The permissions users have once accessing a network and therefore the procedures that verify however and wherever information is also keep or shared all be this umbrella. Disaster recovery and business continuity outline however a company responds to a cyber-security incident or the other event that causes the loss of operations or information. Disaster recovery policies dictate however the organization restores its operations and data to come to a similar operative capability as before the event. Business continuity is that the set up the organization falls back on whereas attempting to work while not sure resources. End-user education addresses the foremost unpredictable cyber-security factor: folks. Anyone will accidentally introduce an outbreak to Associate in Nursing otherwise secure system by failing to follow smart security practices. Teaching users to delete suspicious email attachments, not enter unidentified USB drives, and varied different necessary lessons is important for the safety of any organization. Cyber security refers to the body of technologies, processes, and practices designed to shield networks, devices, programs, and information from attack, damage, or unauthorized access. Cyber security may additionally be noted as data technology security. Cyber security is vital as a result of government, military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of knowledge on computers and different devices. a major portion of that information is sensitive data, whether or not that be belongings, money information, personal data, or different forms of information that unauthorized access or exposure might have negative consequences. Organizations transmit sensitive information across networks and to different devices within the course of doing businesses, and cyber security describes the discipline dedicated to protective that data and therefore the systems wont to method or store it. Because the volume and class of cyber attacks grow, corporations and organizations, particularly those who ar tasked with safeguarding data regarding national security, health, or money records, got to take steps to shield their sensitive business and personnel data. As early as March 2013, the nation's high intelligence officers cautioned that cyber attacks and digital spying ar the highest threat to national security, eclipsing even coercion.

4. TRENDS CHANGING CYBER SECURITY

Here mentioned below area unit a number of the trends that area unit having a large impact on cyber security.

4.1 net servers:

The threat of attacks on net applications to extract information or to distribute malicious code persists. Cyber criminals distribute their malicious code via legitimate net servers they've compromised. however data-stealing attacks, several of that get the eye of media, also are a giant threat. Now, we'd like a larger stress on protective net servers and net applications. net servers area unit particularly the simplest platform for these cyber criminals to steal the information. thence one should always use a safer browser particularly throughout necessary transactions so as to not fall as a prey for these crimes.

4.2 Cloud computing and its services

These days all tiny, medium and huge firms area unit slowly adopting cloud services. In different words the globe is slowly moving towards the clouds. This latest trend presents a giant challenge for cyber security, as traffic will go around ancient points of review. in addition, because the variety of applications offered within the cloud grows, policy controls for net applications and cloud services will ought to evolve so as to stop the loss of valuable data. although cloud services area unit developing their own models still tons of problems area unit being referred to concerning their security. Cloud might offer huge opportunities however it must always be noted that because the cloud evolves therefore as its security considerations increase.

4.3 APT's and targeted attacks

APT (Advanced Persistent Threat) could be a whole new level of cyber crime ware. For years network security capabilities like net filtering or IPS have compete a key half in distinctive such targeted attacks (mostly when the initial compromise). As attackers grow bolder and use additional obscure techniques, network security should integrate with different security services so as to notice attacks. Hence one should improve our security techniques so as to stop additional threats coming back within the future.

4.4 Mobile Networks

Today we have a tendency to area unit able to connect with anyone in any a part of the globe. except for these mobile networks security could be a terribly huge concern. of late firewalls and different security measures have become porous as individuals area unit exploitation devices like tablets, phones, PC's etc all of that once more need further securities excluding those gift within the applications used. we have a tendency to should always place confidence in the safety problems with these mobile networks. additional mobile networks area unit extremely vulnerable to these cyber crimes tons of care should be taken just in case of their security problems.

4.5 IPv6: New web protocol

IPv6 is that the new web protocol that is exchange IPv4 (the older version), that has been a backbone of our networks generally and also the web at massive. protective IPv6 isn't simply a matter of porting IPv4 capabilities. whereas informaticsv6 could be a wholesale replacement in creating additional IP addresses offered, there area unit some terribly elementary changes to the protocol which require to be thought of in security policy. thence it's continually higher to modify to IPv6 as presently as attainable so as to scale back the risks relating to cyber crime.

4.6 cryptography of the code

Encryption is that the method of encryption messages (or information) in such some way that eavesdroppers or hackers cannot browse it.. In anencryption theme, the message or data is encrypted exploitation associate degree cryptography rule, turning it into associate degree illegible cipher text. this is often sometimes through with the utilization of associate degree cryptography key, that specifies however the message is to be encoded. cryptography at a really starting level protects information privacy and its integrity. however additional use of cryptography brings additional challenges in cyber security. cryptography is additionally wont to defend information in transit, as an example information being transferred via networks (e.g. the net, e-commerce), mobile telephones, wireless microphones, wireless intercoms etc. thence by encrypting the code one will understand if there's any outflow of data.

5. ROLE OF SOCIAL MEDIA IN CYBER SECURITY

As we have a tendency to become a lot of social in associate progressively connected world, corporations should realize new ways to safeguard personal info. Social media plays a large role in cyber security andwill contribute plenty to nonpublic cyber threats. Social media adoption among personnel is skyrocketing so is that the threat of attack. Since social media or social networking sites square measure almost utilized by most of them each day it's become a large platform for the cyber criminals for hacking non-public info and stealing valuable information. In a world wherever we're fast to administer up our personal info, corporations need to guarantee they're even as fast in distinguishing threats, responding in real time, and avoiding a breach of any kind. Since individuals square measure simply attracted by these social media the hackers use them as a bait to get {the information|the knowledge|the information} and therefore the data they need. Hence individuals should take applicable measures especially in coping with social media so as to prevent the loss of their info. The ability of people to share info with associate audience of millions is at the guts of the particular challenge that social media presents to businesses. additionally to giving anyone the power to distribute commercially sensitive information, social media conjointly offers constant power to unfold false info, which might be just being as damaging. The speedy unfold of false info through social media is among the rising risks known in world Risks 2013 report. Though social media may be used for cyber crimes these corporations cannot afford to prevent using social media because it plays a crucial role in promotional material of an organization. Instead, they must have solutions that may send word them of the threat in order to repair it before any real injury is finished. However corporations ought to perceive this and recognised the importance of analysing the information particularly in social conversations and provide applicable security solutions in order to remain off from risks. One should handle social media by victimization bound policies and right technologies. Since social media or social networking sites square measure almost utilized by most of them each day it's become a large platform for the cyber criminals for hacking non-public info and stealing valuable information. In a world wherever we're fast to administer up our personal info, corporations need to guarantee they're even as fast in distinguishing threats, responding in real time, and avoiding a breach of any kind. Since individuals square measure simply attracted by these social media the hackers use them as a bait to get

6. CYBER SECURITY TECHNIQUES

6.1 Access management and word security

The conception of user name and word has been basic manner of protective our information. this might be one in all the primary measures relating to cyber security.

6.2 Authentication of information

The documents that we have a tendency to receive should be authenticated be before downloading that's it should be checked if it's originated from a trusted and a reliable supply which they're not altered. Authenticating of those documents is usually done by the opposing virus code gift in the devices. therefore a decent opposing virus code is also essential to shield the devices from viruses.

6.3 Malware scanners

This is code that typically scans all the files and documents gift within the system for malicious code or harmful viruses. Viruses, worms, and Trojan horses square measure samples of malicious code that square measure typically sorted together and cited as malware.

6.4 Firewalls

A firewall may be a code program or piece of hardware that helps separate hackers, viruses, and worms that attempt to reach your laptop over the web. All messages getting into or going the internet experience the firewall gift, which examines every message and blocks those that don't meet the required security criteria. Hence firewalls play a very important role in detecting the malware.

6.5 Anti-virus code

Antivirus code may be a computer virus that detects, prevents, and takes action to disarm or remove malicious code programs, such as viruses and worms. Most antivirus programs include Associate in Nursing auto-update feature that allows the program to transfer profiles of recent viruses therefore that it will check for the new viruses as shortly as they are discovered. Associate in Nursing opposing virus code may be a must and basic necessity for each system.

7. CYBER ETHICS

Cyber ethics area unit nothing however the code of the internet. once we apply these cyber ethics there area unit smart possibilities folks victimisation the net in a correct and safer means. The below area unit a couple of of them:

1. DO use the net to speak and move with others. Email and instant electronic messaging build it simple to stay in-tuned with friends and family members, communicate with work colleagues, and share concepts and information with folks across city or halfway round the world

2. Don't be a bully on the net. Do not call folks names, slug them, send embarrassing photos of them, or do anything else to do to harm them.

3. Web is taken into account as world's largest library with data on any topic in any bailiwick, thus victimisation this information in a very correct and legal means is always essential.

4. Don't operate others accounts victimisation their passwords.

5. Ne'er try and send any quite malware to other's systems and build them corrupt.

6. Ne'er share your personal data to anyone as there's a decent likelihood of others misusing it and eventually you would find yourself in a very bother.

7. Once you're on-line ne'er fake to the other person, and ne'er try and produce fake accounts on some other person because it would land you also because the different person into bother.

8. forever adhere to proprietary information and transfer games or videos provided that they're permissible.The higher than area unit a couple of cyber ethics one should follow whereas victimisation the net. we have a tendency to area unit forever thought correct rules from out terribly early stages the same here we have a tendency to apply in cyber house.

8. CONCLUSION

Computer security could be a huge topic that's becoming additional vital as a result of the planet is becoming extremely interconnected, with networks being used to hold out important transactions. Cyber crime continues to diverge down totally different paths with every year that passes so does the protection of the data. The latest and tumultuous technologies, together with the new cyber tools and threats that return to light-weight every day, area unit difficult organizations with not solely how they secure their infrastructure, but how they need new platforms and intelligence to do so. There's no excellent resolution for cyber crimes however we should always strive our limit to minimize them so as to possess a secure and secure future in cyber area.

12. ACKNOWLEDGEMENT

I am pleased to present “a study of cyber security challenges and its emerging trends on latest technologies” project and take this opportunity to express our profound gratitude to all those people who helped us in completion of this paper. I thank our college for providing us with excellent facilities that helped us to complete and present this paper. I would also like to thank our guide Asst. Prof. Gauri Ansurkar for permitting us to use computers in the lab as and when required for research. I express my deepest gratitude towards our project guide for her valuable and timely advice during the various phases in our project. I would also like to thank her for providing us with all proper facilities and support as the co-coordinator. I would like to thank her for support, patience and faith in our capabilities and for giving us flexibility in terms of working and reporting schedules.

13. 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 Organizations – A Net Action Report by Audrie Krause.

AUTHOR

Name: Dhiraj Yuvraj Bhosale

B.Sc. (Computer Science)

Pursuing M.Sc. (Information Technology)