IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cyber Security: A Crucial Aspect Of The Information Age

Dr. Sanatan Deep
Assistant Professor
Head of the Department of Music
Jamshedpur Women's University

Abstract

Cyber Security is the practice of protecting critical systems and sensitive information systems from digital attacks. Also known as information technology (IT) security, cyber security measures are designed to combat threats against network systems and applications, whether those threats originate from inside or outside of an organisation. In 2020, the average cost of a data breach was USD 3.86 million globally and USD 8.64 million in the United States. These costs include the expenses of discovering and responding to the breach because of downtime and lost revenue, and the long-term reputational damaged to a business and its brand. Cybercriminals target customers' personally identifiable information (PII) - name, addresses, national identification number (e.g., Social Security number in the US, fiscal codes in Italy), and credit card information - and then sale these records in underground digital marketplaces. Compromised PII often leads to a loss of customer trust, the imposition of regulatory fines, and even legal action. Security system complexity, created by disparate technologies and a lack of in- house expertise, can amplify these costs. But organizations with a comprehensive cyber security strategy., governed by best practices and automated using advance analytics, artificial intelligence (AI) and machine learning, can fight cyber threats more effectively and reduce the lifecycle and impact of breaches when they occur. Cyberspace is becoming more complex and we need continuous innovation to keep the space secure and resilient to threats. Indigenous solutions, in-house expertise and startup eco-system needs to be created to reduce dependence on foreign products and solutions for securing our critical infrastructure and defense installations. National Cyber Security Coordinator Dr Gulshan Rai stressed in a conference of cyber security upon the areas of strategic importance including Artificial Intelligence, Robotics, Virtual reality & augmented reality, Internet of things (IOT) which would be the backbone of the country in future.

Kerywords: Cybersecurity, Cyberspace, Information Technology

Introduction

Cyber Security 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 cyber Security 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**).

The Internet is today's fastest growing infrastructure. In today's technical environment many new technologies are changing mankind. But due to these emerging technologies, we are unable to protect our private information in an efficient way, so the cyber-crimes are drastically increasing on daily basis. Majority of the transactions both commercial and personal are done using the means online transaction, so it is important to have an expertise who require a high quality of security maintaining a better transparency to everyone and having safer transactions. So cyber Security is the latest issue. Advanced technologies like cloud services, mobiles, E-commerce, internet banking and many more they require a high standards and safer process of security. All the tools and technologies involved for these transactions hold the most sensitive and cruicial user information. So providing the necessary security to them is very important. Improving the cyber security and safeguarding the sensitive data and infrastructures are important to every countries top priority security (**Panchanatham, 2015).**

Cyber is a prefix derived from the word cybernetics and has acquired the general meaning of through the use of a computer which is also termed as cyberspace. The word security in general usage is synonymous with being safe, but as a technical term security means not only that something is secure, but that it has been secured. Joining the two words together form the word cybersecurity is concerned with making cyberspace safe from threats, namely cyber threats. The information and communications technology (ICT) industry has evolved greatly over the last half century. With the advent of the internet, security becomes a major concern. ICT devices and components are generally inter dependable and vulnerable to the security attacks. The act of protecting ICT systems and their contents has come to be known as cybersecurity. Cybersecurity is an important tool in protecting and preventing unauthorized surveillance. As commonly used, the term cybersecurity refers to three things:

1. A set of activities and other measures, technical and non-technical, intended to protect computers, computer networks, related hardware and devices software, and the information they contain and communicate, including software and data, as well as other elements of cyberspace, from all threats, including threats to the national security.
2. The degree of protection resulting from the application of these activities and measures.
3. The associated field of professional endeavor, including research and analysis, aimed at implementing and those activities and improving their quality.

What is a Cyber Attack

A Cyber attack is where an attackers tries to gain unauthorized access to an IT system for the purpose of theft, extortion, disruption, or other nefarious reasons. Of course, a large number of security incidents are caused by insiders- whether through negligence or malice. However, for the sake of simplicity, let's assume that a cyber – attack is carried out by someone who is not, or was not, a member of our organization.

15 Common Types of Cyber Attacks

While there are many different way that an attackers can infiltrate an IT system, most cyber attacks rely on pretty similar techniques. Below are some of the most common types of Cyber attacks.

1. Malware
2. Phishing
3. Man-in-the-middle-attack (MITM)
4. Distributed Denial attack (MITM)
5. SQL injection
6. Zero-day exploit
7. DNS Tunneling
8. Business Email Compromise (BEC)
9. Cryptojacking
10. Drive- by Attack
11. Cross-site scripting (XSS) attacks
12. Password Attacks
13. Eavesdropping Attacks
14. Al-Powered Attacks
15. IoT –Based Attacks

Indian Cyber Situation

- India ranks 3rd in terms of the highest number of internet users in the world after USA and China, the number has grown 6-fold between 2012-2017 with a compound annual growth rate of 44%.
- India secures a spot amongst the top 10 spam-sending countries in the world alongside USA
- India was ranked among the top five countries to be affected by cybercrime, according to a 22 October report by online security firm ”Symantec Corp.**”**

Top Six Biggest Ransomware Attacks in India

Accoding to **The Indian Express,** ransomware attacks worldwide have **increased by 102% in 2021 compared to 2020.** The resurging ransomware attacks in India has become a headache for the corporate sectors. The attack vector is targeting and affecting various organizations across the nation. Infect, in recent times the three most notorious members of the ransomware family – Ryuk, Purga, and Stop made major headlines in the nation.

The Stop ransomware caused about 10.10% of the ransomware attacks followed by Ruyk making about 5.84% attacks along with Purga for deploying 0.08% of ransomware attacks !

(***Source : TGS Sunday Guadian Live***)

1. **Telangana and AP Power Utilities Hacked –** A malicious software attacked the power Utility system of Telangana and Andhra Pradesh last year where all te servers went down until the glitch was rectified. Since the computer systems of Telangana and Andhra Pradesh power utilities were interlinked, the virus attack quickly spread, taking down all the systems.
2. **UHBVN Ransomware Attack-** Uttar Haryana Bijli Vitran Nigam was hit ny a ransomware attack where the hackers gained access to the computer system of the power **company and stole the billing data of customers. The attackers demanded Rs. 1 crore in return for giving back the data .**
3. **WannaCry –** India was the third worst-hit nation by WannaCry ransomware , **affecting more than 2 lakh computer system.** During the first wave of attacks, tjis ransomware attack had hit banks in India including few enterprises in Tamil Nadu and Gujrat. The ransomware majorly affected the US healthcare system and a well-known French car manufacturing firm.
4. **Mirai Botnet Malware Attack –** This botnet malware took over the internet, targeting home routers and IoT devices. This malware affected **2.5 million IoT devices including a large number of computer system in India.** This self-propagating malware was capable of using exploitable unpatched vulnerabilities to access networks and system.
5. **BSNL Malware Attack** – The state –owned telecom operators BSNL was hit by a mojor malware attack, **Impacting nearly 2000 broadband modems! 60,000 modems became dysfunctional after the malware attack** hit the Telecom Circle.
6. **Petya – India was one of the top 10 countries to be hit by Petya ransomware .** This ransomware attack halted work at one of the terminals of India’s largest seaport causing computer lockdown and serious consequence for the country’s exports.

Approaches to alleviate Cyber Threats

Network Security – Protect your networks against external and internal attack. Manage the network primer. Filter out unauthorized access and malicious contents. Monitor and test security controls

Malware Protection - Produce relevant policy and establish anti-malware defenses that are applicable and relevant to all business areas. Scan for malware across the Organization.

Monitoring - Establish a monitoring strategy and produce supporting policies. Continuously monitor all ICT system and networks. Analyse logs for unusual activity that could indicate an attack.

Incident Management- Establish an incident response and disaster recover capability. Produce and test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to law enforcement.

User Education and Awareness- Produce user policies covering acceptable and secure use of the organization's systems. Establish a staff training programme. Maintain user awareness of the cyber risks.

Home and Mobile Working- Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline to all devices. Protect data both in transit and at rest

Secure Configuration- Apply security patches and ensure that the secure configuration of all ICT systems is maintained. Create a system inventory & define a base line build for all ICT devices.

Removable Media Controls- Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before imported on the corporate system

Managing User Privileges- Establish account management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Information Risk Management Regime- Establish and effective governance structure and determine your risk appetite. Maintain board's engagement with cyber risk. Produce supporting information risk management policies.

Cyber Security Planning

Cyber Trust Layer (1) - Organization heads meet and discuss the criteria for their mutual cyber trust. Network vulnerabilities will be ranked by these criteria

Cyber Impact Layer (2) - Organization heads meet and discuss how their mutually agreed upon criteria will affect their cyber risk. The result drives criteria weights

Cyber Analytic Layer (3) - Cyber security researchers develop a set of custom scientific metrics to assess the Global Severity of identified network vulnerabilities which are ranked by the agreed upon criteria

Cyber Metric Implementation Layer (4) - Cyber security researchers meet with network engineers to develop continuous monitoring framework to identify vulnerabilities and to calculate metrics

Cyber Evaluation Layer (5) - Organization heads meet to discuss their individual Cyber

Maturity and to determine the minimum risk-level necessary for collaboration

Conclusion:

Organizations are finding themselves under the pressure of being forced to react quickly to the dynamically increasing number of cybersecurity threats. Since the attackers have been using an attack life cycle, organizations have also been forced to come up with a vulnerability management life cycle. Cybersecurity is a vast topic that is becoming more important because the world is becoming highly interconnected, with networks being used to carry out critical transactions. Cyber crime continues to diverge down different paths with each New Year that passes and so does the security of the information. The latest and disruptive technologies, along with the new cyber tools and threats that come to light each day, are challenging organizations with not only how they secure their infrastructure, but how they require new platforms and intelligence to do so. There is no perfect solution for cyber crimes but we should try our level best to minimize them in order to have a safe and secure future in cyber space.

References:-

- ibm. Com/in-an/topics/cybersecurity
- Basic Research in Cybersecurity- **MINISTRY OF SCIENCE AND TECHNOLOG**
- Cybersecurity in India: An Evolving Concern for National Security
  Sushma Devi Parmar (Central University of Gujarat)
- Government of India
  Ministry of Defence
  29 OCT 2018 6:29PM by PIB Delhi
- Lepide ,Blog, Data Security, Brian jefferson
- https://www.cyberdegrees.org/resources/hot-technologies-cyber-security/
- Conference on Cyber Security – Challenges and Innovations
- Kratical Blog, July 19, 2021
- Cyber Security Rohit, KALAKUNTLA, Information Technology, University of the Cumberlands, USA
- https://subscription.packtpub.com/book/security/9781788475297/15/ch15lvl1sec101/conclusion
- A STUDY OF CYBER SECURITY CHALLENGES AND ITS EMERGNING TRENDS ON LATEST TECHNOLOGIES G.NIKHITA REDDY1 , G.J.UGANDER REDDY2