Analyzing Cyber Security Issues and Its Impact on the Latest Technologies

[1]Prasun Roy, [2]Samriddha Bhattacharyya, [3]Anirban Bhar, [4]Moumita Ghosh

[1,2] B. Tech student, Department of Information Technology, Narula Institute of Technology, Kolkata, India.
[3,4]Assistant Professor, Department of Information Technology, Narula Institute of Technology, Kolkata, India.

***Abstract*—Within the sphere of knowledge technology, cyber security is crucial. Due to the exponential growth of online threats and attacks, cyber security is currently the most pressing issue. Attackers are increasingly concentrating on the systems with more advanced methods. Numerous layers of defense are scattered throughout the networks, computers, programs, and information that one wants to protect safe from harm in an efficient cybersecurity strategy. Small-scale businesses, huge organizations, and individuals are all affected. Cyber security is important to protect from cybercrimes, which are growing significantly every day. To stop this type of cybercrime, various governments and corporations take various precautions. Numerous steps have been taken to protect against it understanding the extreme concern in the cyber world. So, both IT and non-IT companies have recognized the value of cyber security and are experts in implementing every tool at their disposal to combat online dangers.**

***Keywords*—Cyber Security, Cyber Crime, Attacks, Threats.**

I. INTRODUCTION

Today, a person can send and receive any type of data via email, audio, or video with the simple press of a button, but has he ever considered how securely his data is being delivered to the other person without any information being leaked? Cybersecurity has the solution. The infrastructure of modern living that is rising the fastest is the internet. Many of the most recent technologies are altering the face of humanity in today's technological environment. Sensitive data has been stored as a result of the digitization process in all spheres of human existence, including business, education, healthcare, and others. The technique of keeping digitized information safe from physical harm or theft while retaining its secrecy and accessibility is known as security, but as technology advances quickly, so do the frequency and complexity of cybercrimes. The use of inadequate software, out-of-date security technologies, design flaws, programming errors, readily accessible online hacking tools, a lack of public knowledge, high rates of financial return, etc., are some of the factors contributing to this enormous surge in cybercrime. More potent attack tools are required to investigate the target's weaknesses and ultimately assault the victim. However, because of this new technology, we are unable to effectively protect our private information, which is why cybercrime is on the rise right now. Today, more than 60% of all business transactions are completed online. Today, more than 60% of all business transactions are conducted online, necessitating a high level of security in this sector to provide the most efficient and transparent operations. Thus, cyber security has emerged as a current concern. The scope of cyber security includes many additional areas, such as cyber space, in addition to only protecting data in the IT business.

II. CYBER SECURITY

In order to cover the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including network operations, information assurance, enforcement, etc., cyber security is primarily about people, processes, and technologies working together. In order to protect networks, computers, programs, and data from attack, damage, or illegal access, a variety of technologies, procedures, and best practices have been developed.

- The term cyber security refers to techniques and practices designed to shield digital data.
- The information that's stored, transmitted or used on a data system.

Without a doubt, the cybersecurity technology facilitates our work by ensuring the accessibility of the restricted capital in any network. If a company or society is not honest about the security of its internet activity, they risk looking very bad. Everyone benefits from progressive cyber defense initiatives in the connected world of today. A cybersecurity outbreak might, on a different level, result in everything from identity theft to extortion attempts to the loss of crucial information like family photos. Everyone is reliant on dangerous infrastructure, including hospitals, power plants, and financial service providers. To believe that our civilization is functioning, it is crucial to secure this and other societies.

III. VARIOUS CYBER SECURITY TECHNIQUES

By utilizing new methods, cyberattacks in cyberspace have the potential to increase. To exploit brand-new technical flaws, cybercriminals will most usually update the malware signatures that are currently in use. In other cases, they genuinely look for unique characteristics of cutting-edge technology to identify malware injection flaws. Cybercriminals are gaining access to a large number of people quickly and simply using these new technologies by utilizing emerging Internet technology and millions and billions of active users.

Access Control and Password: A quick and easy way to protect private information and maintain privacy is by using username and password security. One of the most important cyber security initiatives is this kind of security provision.
Authentication: The source of the sent information must be verified as coming from a reliable, unaltered source until then. A gift from the opposing virus software product installed in computers is frequently used to validate these documents. To defend devices from infections, a package of genuinely anti-virus software is more crucial.
Malware Protection: a piece of software that periodically checks the entire system's files and documents for viruses or other malicious code. In this sector, samples of dangerous software systems are typically sorted and labelled as malware by Trojan horses, worms, and viruses.
Firewall: A firewall is a piece of hardware or software that prevents viruses, worms, and hackers from accessing your computer through the internet. The firewall examines each message that enters and rejects any that don't adhere to the standards for universal message security. Firewalls are essential for detecting malware.
Currently, cyber security is a topic of intense discussion in the media, government, and organizations. According to experts, the subject has been exaggerated and artificially inflated by the fear industry, with terminology like "cyber-warfare" meant to elicit an emotional rather than a logical reaction. In a recent analysis by Intelligence, the threat posed by cyberwar has been vastly overblown, with a threat number like 23. The main ideas under discussion on the subject of cyber security might encourage specialists and researchers to think independently. Indeed, many people who advocate caution, such as security professionals, have made this type of conversation a suggestion.These arguments underline the fact that, as opposed to the absence of governmental rules, a significant proportion of cybercrimes are a direct outcome of insufficient security. It is not advisable, according to the president of the Electronic Privacy Information Center, to make online users identify themselves. He cited those nations where the need for accountability led to censorship and transnational human rights abuses. Regardless of the perspective, it is obvious that cyber-security is acknowledged as a crucial and timely issue that is conducive to discussion. This work provides an established, broad definition of cyber-security for the online environment and makes some suggestions for its incorporation in information-related activities [1].Technology programs are built on several public research reports and documentation. Governments and security groups all over the world are adopting proactive measures to lessen the danger of successful assaults against vital infrastructures as the frequency of cyber-attacks rises steadily. It refers to the connection between the physical and digital worlds. Protecting that infrastructure through cyber security involves preventing, identifying, and responding to cyber incidents [2].
The defense mechanism mainly concerns with the understanding of their own network, nature of the attacker, inspire of the attacker, method of attack, security weakness of the network to mitigate future attacks.[3]A cyber-attack is when someone gain or attempts to gain unauthorized access to a computer maliciously [4].

IV. Parameters and Action

1. Identify threats
2. Identify vulnerabilities
3. Access risk explore
4. Establish contingency plan
5. Respond to cyber security accident.

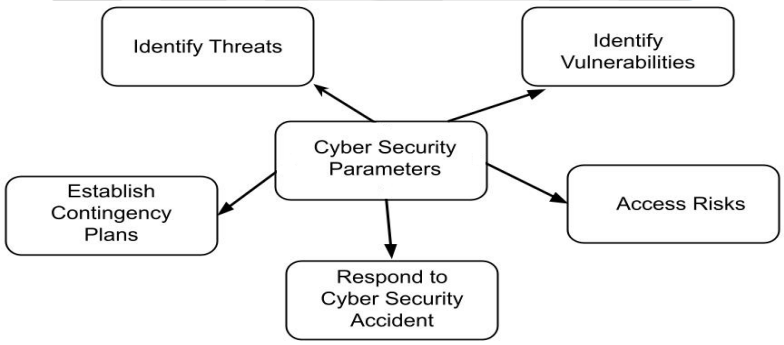

Figure 1: Cyber Security Parameters

We can better understand the motives and behaviors of the attackers by using the categories of cyber-attackers. Operational cyber security risks can result from three different sorts of actions, as depicted in Figure: I) unintentional, unintentional actions (typically by insiders); II) deliberate, intentional actions (typically by insiders or outsiders); and III) inaction (typically by insiders), such as a failure to act in a given situation due to a lack of appropriate skills, knowledge, guidance, or the availability of the correct person to take action. Here, deliberate actions of which there are three types are the main focus are of interest.

1. Political motivations: examples include destroying, disrupting, or taking control of targets; espionage; and making political statements, protests, or retaliatory actions.

2. Economic motivations: examples include theft of intellectual property or other economically valuable assets (e.g., funds, credit card information); fraud; industrial espionage and sabotage; and blackmail.

3. Socio-cultural motivations: examples include attacks with philosophical, theological, political, and even humanitarian goals. Socio-cultural motivations also include fun, curiosity, and a desire for publicity or ego gratification.

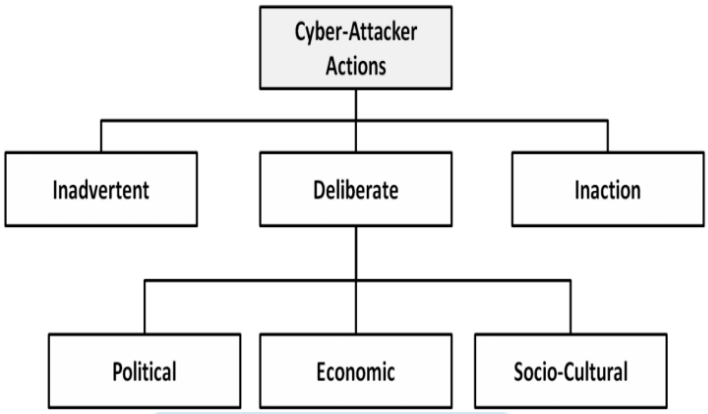

Figure 2: Cyber-Attacker Actions

V. Security Attacks

Security attacks are defined as attempts to gain unauthorized access to information resources or services or to injure or damage information systems.*Denial of Service Attacks*: When numerous systems overload the targeted system's bandwidth, this form of attack is concerned with those systems. This assault causes the system or network to shut down, rendering it unavailable to users. A firewall or other detection system can be used to monitor network traffic in order to identify this kind of attack. It can also be avoided by restricting the number of requests made to a service that is currently in use.*Exhaustive Search Attack:* The fact that the attackers submit a variety of passwords or usernames before selecting one as the right password makes this attack extremely concerning. This occurs as the attacker methodically keeps track of all potential passwords and checks each one until the right one is discovered. The Administrator must forbid the use of some widely used passwords and must instead employ the most unpredictable passwords in order to prevent such assaults.*Portal Attacks:* This kind of attack works regardless of the existence of different web applications and enables an attacker to tamper with the data transmitted from the user's browser to the server. By intercepting a user's traffic to a banking life, these attacks aim to steal financial information.*Shell Shock Attacks*: This attack takes advantage of a flaw in the widely used UNIX command execution shell bash (Bourne-Again Shell), which might allow attackers to take over the computer and remotely run code into the system.

VI. Future Scope and Conclusion

Artificial intelligence, or AI, is currently the technology that is most commonly utilized to ensure cyber security. Robots no longer employ AI exclusively to perform our home chores, like mowing the lawn, for humans. Artificial intelligence tools are rapidly being used by both cybersecurity professionals and hackers. Future cybersecurity will rely heavily on AI.Heuristic algorithms are used by AI to quickly analyses massive volumes of data and find patterns. In order to swiftly uncover vulnerabilities, they may exploit, hackers are now using AI techniques to examine data that has already been obtained, such as network traffic and password credentials. AI is being used by cybersecurity teams to analyze network traffic and data collected by their defense systems in an effort to find new attack patterns and early signs of cyberattacks.The use of artificial intelligence (AI) are transforming how organizations run and interact. One of its most important advantages is its potential to alter cyber security systems and the ability of artificial intelligence to completely secure any cyber information used by businesses. The field of cybersecurity may undergo a transformation thanks to artificial intelligence (AI). It is an essential tool for seeing dangers and taking action since it can analyze enormous amounts of data and identify patterns that are undetectable to humans.Research shows that a computer savvy user is the most effective defense in cyber security situations including attacks. It is important to take into account the most vulnerable individuals, who are new employees inside an organization, as the attacker is primarily looking for personally identifiable information from people involved. The psychological aspects of user and network vulnerability are further validated by this research. In spite of the fact that technology can help lessen the effects of cyberattacks, this paper's findings suggest that education is the most effective way to change people's behavior and psychological predispositions. Cyberattacks can be lessened, but no definitive answer has yet been offered to deal with these security dangers.

References

[1] Rowe, Dale C., Barry M. Lunt, and Joseph J. Ekstrom. "The role of cyber-security in information technology education." Proceedings of the 2011 conference on Information technology education. ACM, 2011.
[2] “Quick Reference: Cyber Attacks Awareness and Prevention Method for Home Users” International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:9, No:3, 2015.
[3] Al-Mohannadi, Hamad, et al. "Cyber-Attack Modeling Analysis Techniques: An Overview." Future Internet of Things and Cloud Workshops (FiCloudW), IEEE International Conference on. IEEE, 2016.
[4] Quick Reference: Cyber Attacks Awareness and Prevention Method for Home Users” International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:9, No:3, 2015.
[5] https://www.forbes.com/sites/forbesbusinesscouncil/2021/09/23/artificial-intelligence-the-future-of-cybersecurity/
[6] Sheth, Mrs & Bhosale, Sachin & Kurupkar, Mr & Prof, Asst. (2021). Research Paper on Cyber Security. 2021.