IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, April 2023

Overview of Cyber Security

Ujjwal Rao
Student, B. Tech, Department of Computer Science and Engineering
Dronacharya College of Engineering, Gurgaon, Haryana, India

Abstract: *With the rise of technology and the increasing reliance on the internet, cyber threats have become a significant concern for individuals, businesses, and governments alike. Cybersecurity is the practice of protecting computer systems, networks, and sensitive information from unauthorized access, theft, and damage. This research paper aims to explore the concept of cybersecurity, including its definition, importance, types of cyber threats, and techniques to prevent them. The paper also analyzes the impact of cyber threats on different sectors, such as government, finance, healthcare, and education. Additionally, the research examines the role of various stakeholders in ensuring cybersecurity, including individuals, organizations, and governments.*

Keywords: Cybersecurity

I. INTRODUCTION

Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.

What's the best cybersecurity strategy? A strong security infrastructure includes multiple layers of protection dispersed throughout a company's computers, programs and networks. With cyber-attacks occurring every 14 seconds, firewalls, antivirus software, anti-spyware software and password management tools must all work in harmony to outwit surprisingly creative cybercriminals. With so much at stake, it's not hyperbolic to think that cybersecurity tools and experts act as the last line of defense between our most vital information and digital chaos.

We should expect its importance and areas of use to continue to rise, and the more advanced the technology grows, the more widely it will be used. It's already widely utilised in facial recognition and picture recognition in general: nudity filters, document processing, and even surveillance, as well as in content recommendation engines like Instagram, Youtube, Netflix, and Pinterest. As they are given datasets to study and learn, AI systems are increasingly coming up with new antibiotics that are meant to treat specific ailments. It may be possible in the future to further integrate AI into healthcare, using it to diagnose patients and provide treatment for their unique ailment.

We will surely see the rise of self-driving vehicles, since we are now on our approach to entirely automating our transportation systems, with AI systems capable of complicated decision-making much like humans. Machine learning is currently progressing in many parts of our lives, and it will only become more integrated as AI technology advances. The rapid development of technology has revolutionized the way we communicate, work, and conduct business. However, with the benefits of technology come significant risks, primarily in the form of cyber threats. Cyber threats refer to malicious activities that aim to compromise the security and integrity of computer systems and networks. Cybersecurity is the practice of protecting computer systems, networks, and sensitive information from unauthorized access, theft, and damage. The importance of cybersecurity cannot be overstated, as cyber threats pose a significant risk to individuals, organizations, and governments worldwide.

II. SCOPE OF CYBER SECURITY

Cyber Security has become an alarming issue for many organizations all over the world. With the wide set of important data that companies hold has led to malicious activities like hacking, cyber threats, and many more. This has created a very concerning issue on how to protect data from hackers. Therefore, companies today are investing into cyber

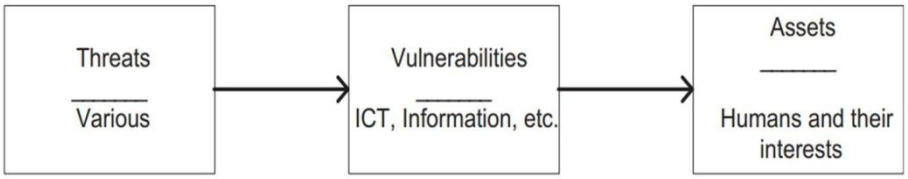
IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, April 2023

security which will help them to shield devices, networks, and programmes from digital attacks is known as cybersecurity.

As the attacks are extremely dynamic, it requires a highly specialized and disciplined approach to tackle with them. Over the years companies have suffered highly insufficient staffing problems and now they are ready to pay more but fortify the security walls. These cyberattacks are usually motivated at gaining access to, altering, or damaging confidential data, extorting money from users and exploiting them, or disrupting normal business processes.

III. HOW DOES CYBER SECURITY WORKS

Cybersecurity is designed to provide multiple layers of protection across all of the computers, networks, and programs used by a business. In order to create a unified defence against potential cyberattacks, it is important that the business, employees, processes, and technology are designed to work seamlessly together. Cybersecurity systems that function properly will be able to detect, investigate, and resolve potential weaknesses and vulnerabilities in the system before they can be exploited by a hacker or malicious software.



3.1 Information Security

The aim of information security is to ensure business continuity and minimise business damage by limiting the impact of security incidents (Von Solms, 1998). Information security can be defined in a number of ways.

The international standard, ISO/IEC 27002 (2005), defines information security as the preservation of the confidentiality, integrity and availability of information (ISO/IEC 27002, 2005, p. 1). In the context of ISO/IEC 27002 (2005), information can take on many forms. It can be printed or written on paper, stored electronically, transmitted by post or electronic means, shown on films, conveyed in conversation, and so forth (ISO/ IEC 27002, 2005, p. 1). Whitman and Mattord (2009) define information security as "the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information" (Whitman and Mattord, 2009, p. 8). These authors (2009) also identify several critical characteristics of information that give it value in organisations

IV. TYPES OF CYBER SECURITY THREATS

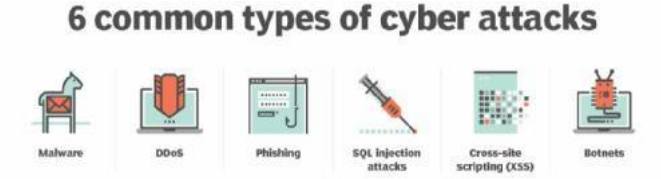
The process of keeping up with new technologies, security trends and threat intelligence is a challenging task. It is necessary in order to protect information and other assets from cyberthreats, which take many forms. Types of cyber threats include:

- Malware is a form of malicious software in which any file or program can be used to harm a computer user. This includes worms, viruses, Trojans and spyware.
- Ransomware is another type of malware. It involves an attacker locking the victim's computer system files -- typically through encryption -- and demanding a payment to decrypt and unlock them.
- Social engineering is an attack that relies on human interaction to trick users into breaking security procedures to gain sensitive information that is typically protected.
- Phishing is a form of social engineering where fraudulent email or text messages that resemble those from reputable or known sources are sent. Often random attacks, the intent of these messages is to steal sensitive data, such as credit card or login information.
- Spear phishing is a type of phishing attack that has an intended target user, organization or business.
- Insider threats are security breaches or losses caused by humans -- for example, employees, contractors or customers. Insider threats can be malicious or negligent in nature.
- Distributed denial-of-service (DDoS) attacks are those in which multiple systems disrupt the traffic of a targeted system, such as a server, website or other network resource. By flooding the target with messages,

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, April 2023

connection requests or packets, the attackers can slow the system or crash it, preventing legitimate traffic from using it.

- Advanced persistent threats (APTs) are prolonged targeted attacks in which an attacker infiltrates a network and remains undetected for long periods of time with the aim to steal data.
- Man-in-the-middle (MitM) attacks are eavesdropping attacks that involve an attacker intercepting and relaying messages between two parties who believe they are communicating with each other.



Other common attacks include botnets, drive-by-download attacks, exploit kits, malvertising, vishing, credential stuffing attacks, cross-site scripting (XSS) attacks, SQL injection attacks, business email compromise (BEC) and zero-day exploits.

V. CYBER SECURITY CHALLENGES

Cybersecurity is continually challenged by hackers, data loss, privacy, risk management and changing cybersecurity strategies. The number of cyberattacks is not expected to decrease in the near future. Moreover, increased entry points for attacks, such as with the arrival of the internet of things (IoT), increase the need to secure networks and devices.

One of the most problematic elements of cybersecurity is the evolving nature of security risks. As new technologies emerge, and as technology is used in new or different ways, new attack avenues are developed. Keeping up with these frequent changes and advances in attacks, as well as updating practices to protect against them, can be challenging. Issues include ensuring all elements of cybersecurity are continually updated to protect against potential vulnerabilities. This can be especially difficult for smaller organizations without the staff or in-house resources.

Additionally, organizations can gather a lot of potential data on individuals who use one or more of their services. With more data being collected, the likelihood of a cybercriminal who wants to steal personally identifiable information (PII) is another concern. For example, an organization that stores PII in the cloud may be subject to a ransomware attack. Organizations should do what they can to prevent a cloud breach.

Cybersecurity programs should also address end-user education, as employees may accidently bring viruses into the workplace on their laptops or mobile devices. Regular security awareness training will help employees do their part in keeping their company safe from cyberthreats.

Another challenge to cybersecurity includes a shortage of qualified cybersecurity personnel. As the amount of data collected and used by businesses grows, the need for cybersecurity staff to analyze, manage and respond to incidents also increases. $(ISC)^2$ estimated the workplace gap between needed cybersecurity jobs and security professionals at 3.1 million.

5.1 Use of Automation in Cybersecurity

Automation has become an integral component to keep companies protected from the growing number and sophistication of cyberthreats. Using artificial intelligence (AI) and machine learning in areas with high-volume data streams can help improve cybersecurity in three main categories:

Threat detection. AI platforms can analyze data and recognize known threats, as well as predict novel threats.

Threat response. AI platforms also create and automatically enact security protections.

Human augmentation. Security pros are often overloaded with alerts and repetitive tasks. AI can help eliminate alert fatigue by automatically triaging low-risk alarms and automating big data analysis and other repetitive tasks, freeing humans for more sophisticated tasks.

Other benefits of automation in cybersecurity include attack classification, malware classification, traffic analysis, compliance analysis and more.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, April 2023

VI. ROLE OF SOCIAL MEDIA IN CYBER SECURITY

As we become more social in an increasingly connected world, companies must find new ways to protect personal information. Social media plays a huge role in cyber security and will contribute a lot to personal cyber threats. Social media adoption among personnel is skyrocketing and so is the threat of attack. Since social media or social networking sites are almost used by most of them every day it has become a huge platform for the cyber criminals for hacking private information and stealing valuable data. In a world where we're quick to give up our personal information, companies haveto ensure they're just as quick in identifying threats, responding in real time, and avoiding a breach of any kind. Since people are easily attracted by these social media the hackers use them as a bait to get the information and the data they require. Hence people must take appropriate measures especially in dealing with social media in order to prevent the loss of their information. The ability of individuals to share information with an audience of millions is at the heart of the particular challenge that social media presents to businesses. In addition to giving anyone the power to disseminate commercially sensitive information, social media also gives the same power to spread false information, which can be just being as damaging. The rapid spread of false information through social media is among the emerging risks identified in

Global Risks 2013 report. Though social media can be used for cyber crimes these companies cannot afford to stop using social media as it plays an important role in publicity of a company. Instead, they must have solutions that will notify them of the threat in order to fix it before any real damage is done. However companies should understand this and recognise the importance of analysing the information especially in social conversations and provide appropriate security solutions in order to stay away from risks. One must handle social media by using certain policies and right technologies.

VII. CYBER SECURITY TECHNIQUES

Access Control and Password Security: The concept of user name and password has been fundamental way of protecting our information. This may be one of the first measures regarding cyber security

Authentication of Data: The documents that we receive must always be authenticated be before downloading that is it should be checked if it has originated from a trusted and a reliable source and that they are not altered. Authenticating of these documents is usually done by the anti virus software present in the devices. Thus a good anti virus software is also essential to protect the devices from viruses.

Malware Scanners: This is software that usually scans all the files and documents present in the system for malicious code or harmful viruses. Viruses, worms, and Trojan horses are examples of malicious software that are often grouped together and referred to as malware.

Firewalls: A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet. All messages entering or leaving the internet pass through the firewall present, which examines each message and blocks those that do not meet the specified security criteria. Hence firewalls play an important role in detecting the malware.

Anti-virus Software: Antivirus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software programs, such as viruses and worms. Most antivirus programs include an autoupdate feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered. An antivirus software is a must and basic necessity for every system.

VIII. CONCLUSION

Computer security 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. Cybersecurity is a crucial aspect of modern-day technology, as cyber threats pose a significant risk to individuals, organizations, and governments worldwide. Cyber threats come in various forms, including viruses,

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, April 2023

malware, phishing attacks, ransomware, and social engineering. Techniques to prevent cyber threats include firewalls, antivirus software, data

REFERENCES

[1]. A Sophos Article 04.12v1.dNA, eight trends changing network security by James Lyne.
[2]. Cyber Security: Understanding Cyber Crimes- SunitBelapure Nina Godbole
[3]. Computer Security Practices in Non Profit Organisations – A NetAction Report by Audrie Krause.
[4]. A Look back on Cyber Security 2012 by Luis corrons – Panda Labs.
[5]. IEEE Security and Privacy Magazine – IEEECS "Safety Critical Systems – Next Generation "July/ Aug 2013.
[6]. CIO Asia, September 3rd , H1 2013: Cyber security in malaysia by Avanthi Kumar.