International Journal of Advance Research in Science and Engineering
Volume No. 12, Issue No. 06, June 2023
www.ijarse.com
IJARSE
ISSN 2319 - 8354

EVALUATION OF CYBER SECURITY DIFFICULTIES AND NEW TRENDS IN LATEST TECHNOLOGIES

P. Ramanjaneya Prasad[1], B. Durga Neelima[2]

[1] *Assistant Professor, Department of Computer Science, Avanthi Degree & PG College, Osmania University, Hyderabad, India.*

[2] *Assistant Professor & Head, Department of Computer Science, Avanthi Degree & PG College, Osmania University, Hyderabad, India.*

ABSTRACT

Modern India places a great emphasis on science and technology, knowing that it is a critical component of economic progress. It has emerged as the global leader in digital services made available to citizens via better online infrastructure and high-speed internet connectivity, transforming the country into Digital India. According to a recent analysis by the United States Federal Bureau of analysis (FBI), India ranks fourth on the list of countries afflicted by cybercrime. Various governments and businesses are taking numerous steps to combat cybercrime. Everyone is still unable to comprehend it. This presentation focuses on the progress of cyber security and the importance of protecting all forms of data against theft and loss. The major obstacles in cybersecurity and the deployment of cybersecurity solutions in accordance with ethical principles, while on the other hand, the risk resides in human and psychology behaviour, which may result in a serious catastrophe

Keywords: *Cyber Security, Cybercrime, Cyber-Attack, Hacking, Ransomware.*

1. INTRODUCTION

Every country in the world is working to digitalize government and commercial sector services. Digital India was launched with an objective of connecting rural areas with high-speed networks and improving digital literacy. Cybercrime is a widespread issue that is making headlines. It endangers individual security and poses an even greater risk to massive international corporations, banks, and governments. Large organised criminal rings today work like start-ups and frequently employ highly-trained coders who are continuously developing online attacks, considerably outnumbering the lone hackers of the past. With so much data available to attack, cybersecurity has become critical. The crime environment in cyber space is totally different from the real space that is why there are many hurdles to enforce the cybercrime law as real space law in any society [1][2].

It is true that today's generation lives on the internet, and most of us are completely unaware of how those random bits of 1's and 0's reach our computer securely. It's a great age for hackers. With so many access points, public IP addresses, and tonnes of data to exploit, black hat hackers are having a difficult time exploiting flaws and developing malicious software. Above that, cyber-attacks are becoming more sophisticated by the day. Hackers' malware is becoming smarter and more inventive, and many people are still perplexed as to how they

avoid virus scans and firewalls. As a result, there must be some kind of mechanism in place to safeguard us from all of these cyber-attacks and ensure that our data does not fall into the wrong hands.

Cyber security implementation includes software, hardware, and human components. Humans must set practises such as using secure passwords and not revealing them, and software must be patched to address weaknesses. Antivirus software and firewalls can assist in preventing unauthorised access to confidential information.

The defence 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].

2. Online Social Media Privacy and Security

We are not unfamiliar with the term "social media." Our daily lives are incomplete; we humans subsist on food, drink, air, and social media. We are so reliant that we tend to divulge every detail about ourselves on social media platforms. However, the main focus should be on whether our data is secure and whether we have any privacy. The majority of users are unaware of the risks and unintentionally give their information, making them vulnerable to cyber-attacks. Social media is the most popular medium for cyber thieves to assault. Cyber security attempts to protect users' personal and professional information against cyber-attacks on the internet.

Though social media might be exploited for cybercrime, these organisations cannot afford to cease using it because it is vital for brand publicity. Instead, they need solutions that will alert them to the threat so that they can solve it before any serious damage is done. Companies, on the other hand, should recognise this and acknowledge the value of assessing information, particularly in social chats, and give suitable security measures to avoid hazards. Certain regulations and technologies must be used to manage social media.

3. Changing Cyber Security Trends

With the Digital Revolution sweeping the globe, all businesses, large and small corporations, organizations, and even governments are relying on computerized systems to manage their day-to-day operations, protecting data from internet assaults and unauthorized access is a significant responsibility for the company. As news of data breaches, ransomware, and hackers become the norm, continuous technological development necessitates a corresponding movement in cybersecurity practices. The different cybersecurity trends in 2023 are listed.

3.1 Rise in Automotive Hacking

Modern automobiles are outfitted with automatic software that allows drivers to stay connected in areas like cruise control, engine timing, door locking, airbags, and advanced driver aid systems. These automobiles connect to the internet via Bluetooth and Wi-Fi, making them vulnerable to security issues and hacking hazards. As more driverless vehicles hit the road in 2023, the usage of microphones for eavesdropping and

gaining control of the vehicle is projected to increase. Self-driving or autonomous vehicles rely on a more complex procedure that necessitates strict cybersecurity measures.

3.2 Artificial Intelligence's Potential (AI)

AI, in conjunction with machine learning, has resulted in significant advancements in cybersecurity, with AI being used across all market sectors. AI has been instrumental in the advancement of automated security systems, natural language processing, face recognition, and autonomous danger detection. It's also being used to create sophisticated malware and attacks that can bypass even the most advanced data protection safeguards. Threat detection systems based on artificial intelligence can forecast future assaults and promptly inform administrators of data breaches.

3.3 The New Target is Mobile

In 2019, cybersecurity trends estimate a 50% increase in mobile banking malware or attacks, making our mobile devices a target for hackers. All of our photographs, financial transactions, emails, and communications put people at risk. In 2023, a smartphone virus or malware could be the focus of cybersecurity developments.

3.4. The Cloud May be Vulnerable as Well

To prevent data breaches as more organisations shift to the cloud, security measures must be examined and enhanced on a regular basis. Even if cloud programmes like Google and Microsoft are well-secured on their end, user mistake, malicious software, and phishing attacks remain a major source of errors, malware, and phishing attacks.

3.5 Data Breach: A High-priority Target

Data will remain a cause of concern for organisations all over the world. Securing digital data is a key concern for both consumers and businesses. Hackers may take advantage of any minor defect or flaw in your system browser or programme to obtain access to personal information.

3.6 Technology and Risks in a New Era: IoT on a 5G Network

With the launch and expansion of 5G networks (IoT), the Internet of Things will usher in a new era of interconnection. This connection across multiple devices exposes them to external influences, assaults, or unknown software flaws. Chrome, the world's most popular browser and a Google product, has also been discovered to contain major flaws. 5G architecture is a new technology on the market that requires substantial research to uncover security weaknesses and make the system safe from external attack. Every level of the 5G network may result in a slew of network attacks that we are absolutely unaware of. Manufacturers must design complicated 5G hardware and software with considerable caution to prevent data leaks.

3.7 Integration and Automation

With the amount of data increasing by the day, it is critical to leverage automation to enable more complex data management. Professionals and engineers are under tremendous pressure to offer rapid and effective solutions in today's demanding work environment, making automation more useful than ever. Security measures are included into the agile process to create more secure software in all aspects. Larger, more complicated web applications are far more difficult to secure, necessitating the inclusion of automation and cyber security as basic concepts in the software development process.

3.8 Ransomware with a Specific Target

Another significant cybersecurity issue that we can't seem to ignore is targeted ransomware. Industries, particularly those in developed countries, rely heavily on specialised software to handle their daily operations.

These ransomware targets are increasingly specific, as seen by the Wanna Cry ransomware attack on NHS hospitals in England and Scotland, which infected over 70,000 medical devices. Though ransomware frequently threatens to expose the victim's data unless a ransom is paid, it can also affect large organisations or countries.

3.9 Cyber Warfare Supported by the Government

There will be no ceasefire between the western and eastern powers in their battle for dominance. Even while such attacks are rare, they have a huge impact on events like as elections, tensions between the United States and Iran, and Chinese hackers. With over 70 elections scheduled this year, criminal activity is projected to rise. High-profile data breaches, as well as political and industrial secrets, are expected to be among the top cybersecurity themes in 2023.

3.10 Threats from Within

Human error is one of the most common causes of data breaches. A single bad day or intentional defect can bring down an entire company, leading in millions of dollars in stolen data. According to a Verizon data breach study that gives strategic insights on cybersecurity trends, employees were directly or indirectly responsible for 34% of overall attacks. As a result, ensure that all employees are aware of the importance of data security in every way.

4. Cybersecurity Tools

A CyberSecurity Software is required for a company's or individual's cyber security and privacy. Cybersecurity is a means of protecting a network, system, or applications from cyber-attacks. It is employed in order to prevent unauthorised data access, cyber-attacks, and identity theft.

The various components of cybersecurity include application security, information security, network security, disaster recovery, operational security, and so on. It must be kept up to date for many forms of cyber threats such as Ransomware, Malware, Social Engineering, Phishing, and so on. The most recent top trending cybersecurity products that will safeguard the entire system from cyber-attacks are highlighted [4].

4.1 SecPod SanerNow

The SanerNow cyber hygiene platform offers an advanced vulnerability management solution to enable continuous security risk management and a compliance posture for cyber-attack prevention. It is a sophisticated vulnerability management technology that combines vulnerability assessment and real-time remediation into a single unified console. It checks for vulnerabilities, misconfigurations, and other issues and provides remediation controls and techniques to automatically and rapidly address them. Every step of vulnerability management, from scanning to remediation, can be automated using its natively developed system. SanerNow assists you in improving your organization's security posture and preventing cyber-attacks.

4.2 Acunetix

Acunetix is the solution to secure your websites, web applications, and APIs. This application security testing solution can find over 7000 vulnerabilities and scan all pages, web apps, and complex web applications. It has built-in vulnerability management functionality. On-premise and on-demand deployment options are available with Acunetix. Acunetix makes use of advanced macro recording technology that will be helpful for scanning complex multi-level forms and password-protected areas of the site. It performs the assessment for the severity of the issue and provides actionable insights immediately. It provides the functionalities for scheduling & prioritizing the full scans/incremental scans.

4.3 Intruder

Comprehensive suite of solutions that are designed to keep Mac and Windows systems safe from all forms of threats. There is an anti-virus solution that renders real-time threat protection. Then we also have the Net Barrier that facilitates advanced firewall protection. There is also a VPN that can be used for internet privacy. Its main features are Ransomware protection, VPN, Advanced Firewall protection, Zero-day protection and Set parental controls

4.4 Perimeter 81

Perimeter 81 is a software programme that immediately drew us over with all of its powerful network security capabilities. The software provides its customers with a slew of cybersecurity solutions to fortify your organization's defences against a wide range of potential threats. The programme streamlines the process of controlling and securing the integrity of your network by including capabilities such as device posture check, web filtering, Zero Trust Network access, and multi-factor authentication.

4.5 Wire shark

It is a network analyzer protocol that is frequently used. It evaluates the vulnerable network segments on which the user is operating. Wireshark can record or view the details and actions that occur on a network. The incoming and outgoing data packets, as well as the protocol utilised in transmission, are plainly visible. It records live data and generates an offline analysis sheet to aid with tracking.

5. Methods for Preventing, Detecting and Responding to Cyber Attacks

- Employee education in cyber security principles.
- Install, utilise, and frequently update antivirus and antispyware software on all work computers.
- For your internet connection, use a firewall.
- Download and install system and application updates when they become available.
- Create backup copies of critical corporate data and information.
- Physical access to your PCs and network components might be restricted.
- Protect your Wi-Fi network. If your office has a Wi-Fi network, ensure sure it is safe and concealed.
- Each employee must have their own user account.
- Limit employee access to data and information, as well as software installation authority. Passwords should be changed on a regular basis.

CONCLUSION

Today, the wisest decision to increase your security is that cyber security training programmes are to be done at the educational, institutional, and industrial levels, which will offer the individual with the essential skills to become an expert in sensing cyber-attacks. One must adopt complete strategies for protecting infrastructures, such as securing data and information, performing risk analysis and mitigation, architecting cloud-based security, achieving compliance, and much more. People must also be aware of cybercrime legislation and the actions that will be taken to combat criminality.

REFERENCES

[1] Razzaq, Abdul, et al. "Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications. “Autonomous Decentralized Systems (ISADS), 2013 IEEE Eleventh International Symposium on. IEEE, 2013

[2] “Digital India” https://en.wikipedia.org/wiki/Digital_India

[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] “Trending top cyber security tools in 2023” https://www.softwaretestinghelp.com/cybersecurity-software-tools/