International Journal of Scientific Research and Engineering Development-– Volume 4 Issue 3, May- June 2021
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

A STUDY OF CYBERSECURITY CHALLENGES AND EMERGING TRENDS ON LATEST TECHNOLOGIES

Pruthviraj Jadhav*

*(High school senior at Maharashtra Kanisht Mahavidyalay, Latur, Maharashtra, India)

Email: pruthvi5533y@gmail.com

----------**********----------

Abstract- In today's world, securing information has become the most significant challenge; that is why cyber security plays an important role. As cybercrimes are increasing day by day, cyber security needs to be updated. This paper mainly focuses on the challenges of cyber security in the latest technology and cyber security tools.

Keywords:- **Cybersecurity, Cybercrime**

----------**********----------

I. INTRODUCTION

Today humans are spending millions of GB data from one place to another throughout the internet. The data can be in the form of email, videos, audios, etc. But how securely is this data being transmitted? Cybersecurity is the answer to this question. As new technologies are emerging, we need strong security to safeguard our private information effectively. Today security is very important as organizations need to defend themself against data breach campaigns, making them an irresistible target for cybercriminals. As fast as security grew, the hacking world grew faster. Cyber threats can come from any level of organization as risk is increasing, driven by global connectivity and usage of cloud services like Amazon web services to store sensitive data and personal information. The widespread poor configuration of cloud services paired with increasingly sophisticated cybercriminals means the risk that the organization suffers from successful cyber attacks or data breach is on the rise. In today's world, it is essential to protect all categories of data from theft and damage.

II. CYBERCRIME

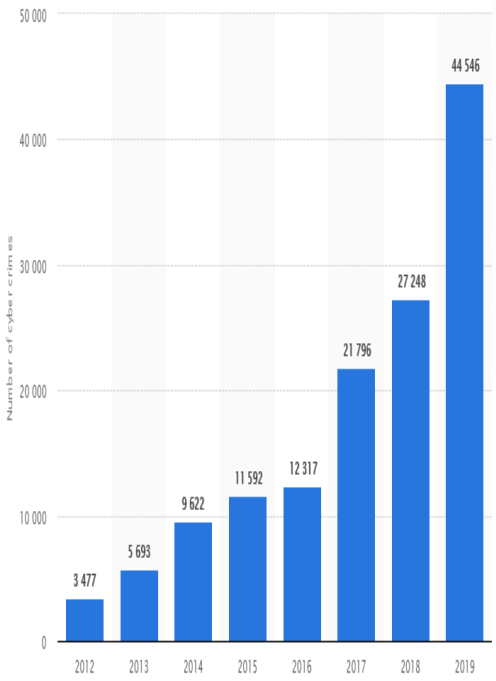
Cyber crime is a criminal activity that either targets or uses a computer, a computer network, or neutral devices. Cyber crime may threaten a prison, company, or nation's security and financial health. Cyber crime includes crimes made possible by computers, such as network intrusions and the dissemination of computer viruses and computer-based variations of existing crimes, such as identity theft, staking bullying, and terrorism, significant problem to people and nation. As day by day, technology is playing an important role in a person's life; cyber crime also will increase along with the technological advances.

III. Cybersecurity / Information technology security

Cybersecurity is the practice of defending computers, servers, mobile devices, electronic system networks, and data from attacks. We are living in a world where all the information is maintained in digital form. It is very important in today's world to keep information safe, as it contains personal information. Cyber attacks are an increasingly sophisticated and evolving danger to your sensitive data, as attackers employ new methods

powered by social engineering and artificial intelligence to traditional security control.

The graph below shows how Cybercrime increased from 2012 -2019 in India.



Government officials and information technology security specialists have documented a significant increase in Internet-based crimes. According to the FBI, IC3 (internet crime complaint center) received 467361 complaints in 2019 - an average of nearly 1300 every day and recorded more than $3.5 billion in losses to individuals and business victims. The most frequently reported complaints were phishing and similar plays, non-payment/non-delivery scams, and extortion.

IV. Cybersecurity trends.

Following are the future trends for 2021.

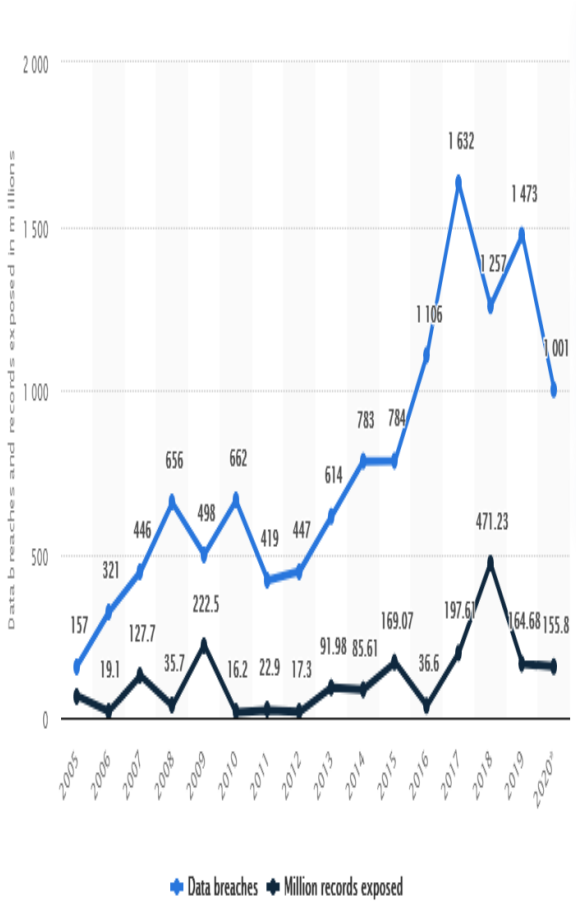
A. Data Breach: Prime target

Data will continue to be a leading concern for organizations worldwide, whether for individuals or organizations. The safety of digital data is the primary goal now. Data breaches can occur in any size of an organization, from small businesses to major corporations. Here are some examples of data breaches,

1) Loss or theft of hard copy notes

2) USB drives

An unauthorized person gaining access to your laptop, email account, or computer network and taking out data is called a data breach.

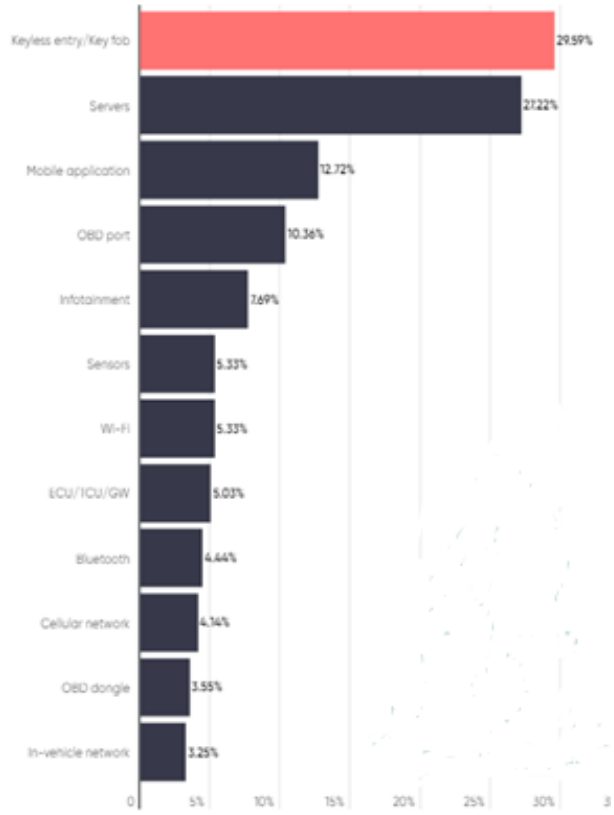


This table shows the annual data breaches and exposed records in the United States from 2005 to 2020.

***B. Automotive Hacking*:-** It is the exploitation of vulnerabilities within the software, hardware, and communication system of automobiles. Modern automobiles contain hundreds of onboard computers processing everything from vehicle control to the informant system. A computer called electronic control units communicates with each other through multiple network and communication protocols, including Controller Area Network (CAN) for vehicle

components communication such as the connection between engine and brake control. Local Internet-connect Network (LIN) for cheaper vehicle component communication between door locks and interior lights ; (MOST) Median oriented system Transport. For information systems such as modern touch screens and telematics connections. Self-driving or autonomous vehicles use an even future complex mechanism that requires strict cybersecurity measures. Gaining control of the vehicle or using microphones for eavesdropping is expected to rise in 2021 with more automated vehicles**.**

*Information: the chart displays most common automotive hacking methods from 2010 to 2020.



C. IoT with 5G Network:-

The next Ranging cyber security trend for 2021 is loT with 5G Networks. 5G networks are expected to roll out in 2020 globally. A new era of interconnectivity will become a reality with the Internet of Things (loT). This communication between multiple devices will open them to vulnerabilities from outside influence, attacks, or an unknown software bug. Even the world's most used browser supported by Google Chrome was found to have serious flaws. 5G architecture is much effectively new in the industry and requires a lot of research to find loopholes to make the system secure from external attacks.

- According to the GSMA, 5G connections are expected to grow from 10 million at the end of 2019 to 1.8 billion by 2025 - and we're well on the way!
- In June 2020, the Global Mobile Suppliers Association (GSA) identified 81 Mobile Network Operators (MNOs) in 42 countries who had launched 5G commercial services. More than 385 MNOs in 125 countries were investing in 5G development.

D. Mobile:-

Mobile device security threats are on the rise. In 2014, Kaspersky detected almost 3.5 million pieces of malware on more than 1 million user devices. By 2017, Kaspersky's in-lab detection technologies processing reached 360,000 malicious files per day. And 78% of those files were malware programs, meaning that over 280,000 malware files per day were detected—many of which target mobile devices. Here's a look at the top seven mobile device threats and what the future holds.

1. Data leakage
2. Unsecured Wi-Fi
3. Network Spoofing
4. Phishing Attacks
5. Spyware
6. Broken Cryptography
7. Improper Session Handling.

V. Cyber security tools

A. Firewalls

As we know, the firewall is the core of security tools, and it becomes one of the most essential security tools. Its job is to prevent unauthorized access to or from a private network. It can be implemented as hardware, software, or a combination of both. The firewall is used to prevent unauthorized Internet users from accessing private networks. All information is entering or leaving through the firewall.

B. Antivirus software:- It is a program that is designed to prevent defects and remove viruses and other malware attacks on the individual computer, network, and its system. It also protects our computers

and networks from various threats and viruses such as Trojan horses, worms, keyloggers, browser hijackers, rootkits, spyware, botnets, adware, and ransomware.

***C. PKI Services* :-** PKI stands for Public Key Infrastructure. This tool supports the distribution and identification of public encryption key. It enables users and computer systems to safely change data over the internet and verify the identity of the other part.

***D. Penetration Testing*:-** Penetration testing or pentest is vital to evaluate our business security system and infrastructure security by safely exploiting vulnerabilities. These vulnerabilities exist in the operating system, services, application, improper configuration, or risky end-user behavior. In penetration testing, cyber security professionals will use the same technique and procedure utilized by criminal hackers to check for potential threats and areas of weakness**.**

***E. Malware scanner* :-** Software that usually scans all files and documents present in the system for malicious code or harmful viruses. Worms and Trojan Horses are examples of malicious software that are often grouped and referred to as malware**.**

***F. Cyber Ethics*:-** Cyberethics is the philosophical study of the ethics of computers, encompassing user behavior, what computers are programmed to do, and how this affects individuals and society. For years, various governments have enacted regulations with the organization have defined policies about cyber ethics. When we practice this cyberethics, there are good chances of using the Internet properly and more safely. Below are a few of them.

- Do not use rude or offensive language.
- Do not cyberbully.
- Do not plagiarize.
- Do not break into someone else's computer.
- Do not use someone else's password.
- Do not attempt to infect or in any way try to make someone else's computer unusable.
- Adhere to copyright restrictions when downloading material from the Internet, including software, games, movies, or music.

VI. *CONCLUSION* :-

Cybercrime continues to diverge down different paths with each New Year that passes, and so does the security of the information. Cybersecurity is an important factor as the world is connecting with each other by internet. Cybersecurity should be improved to secure our future in cyberspace.

REFRENCES:-

[1] https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

[2] https://www.statista.com/statistics/309435/india-cyber-crime-it-act/

[3] https://en.wikipedia.org/wiki/Automotive_hacking

[4] https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120

[5] https://www.upguard.com/blog/cybersecurity-important

[6] https://www.javatpoint.com/cyber-security-tools

[7] upstream.auto

[8] https://www.kaspersky.co.in/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store.

