INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)

Vol. 04, Issue 10, October 2024, pp : 232-238

www.ijprems.com
editor@ijprems.com

e-ISSN : 2583-1062

Impact Factor : 7.001

CYBER SECURITY CHALLENGES AND THREATS

Dr. K. Pavithra[1]

[1]Head Of The Department Department Of B. Com (E. Commerce) Pollachi College Of Arts And Science Poosaripatti, Pollachi.

ABSTRACT

Cyber Security plays an important role in the field of information technology .Securing the information have become one of the biggest challenges in the present day. When ever we think about the cyber security the first thing that comes to our mind is 'cyber crimes' which are increasing immensely day by day. Various Governments and companies are taking many measures in order to prevent these cyber crimes. Besides various measures cyber security is still a very big concern to many. This paper mainly focuses on challenges faced by cyber security on the latest technologies .It also focuses on latest about the cyber security techniques, ethics and the trends changing the face of cyber security.

Keywords: cyber security, cyber crime, cyber ethics, social media, cloud computing, android apps.

1. INTRODUCTION

Cyber Security is a process that's designed to protect networks and devices from external threats. Businesses typically employ Cyber Security professionals to protect their confidential information, maintain employee productivity, and enhance customer confidence in products and services.The world of Cyber Security revolves around the industry standard of confidentiality, integrity, and availability, or CIA. Privacy means data can be accessed only by authorized parties; integrity means information can be added, altered, or removed only by authorized users; and availability means systems, functions, and data must be available on-demand according to agreed-upon parameters.

The technique of protecting internet-connected systems such as computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks is known as cybersecurity. We can divide cybersecurity into two parts one is cyber, and the other is security. Cyber refers to the technology that includes systems, networks, programs, and data. And security is concerned with the protection of systems, networks, applications, and information. In some cases, it is also called electronic information security **or** information technology security**.**

DEFINITION

Cybersecurity is outlined as the practice of forestalling unauthorised approach, misuse, and harm to manipulative structures, networks, dossiers, and certainties. It includes a broad range of plans, forms, and processes booked to protect the solitude, chance, and fullness of mathematical characteristics. Cybersecurity demands preventing, recognizing, and fighting many connected to the internet dangers particular taxicab attempts, malware contaminations, dossier breaches, and additional cybercrimes

2. REVIEW OF LITERATURE

Barker explains that the Trojan backdoor Yebot is capable of implementing many negative actions on an infected machine. It downloads and decrypts the Trojan and transfers control to it after sending a request to the remote server. It will monitor and interfere with surfing, and is also capable of logging keystrokes. Analysts show this as a multiple use malware being used as a banking Trojan.

Cloherty and Thomas discuss a malware program that is a threat to U.S. national security. Sources believe software sponsored by the Russian government is used to control oil and gas pipelines, as well and water and filtration systems. The Department of Homeland Security states that a computer network has been hacked as a threat, but the malware hasn't been activated.

Kaspersky Labs' Global Research and Analysis Team discuss an international science conference in Houston, TX 2009. The Trojan DoubleFantasy sends basic system information to the hackers. This allows them to upload another malware to the victim's machine.

Garnaeva et al observe mobile banking Trojan statistics in 2014. Statistics show that USA is the top country under attack. Russia leads in number of individual users attacked by bank malware. Mobile banking Trojans increased nine times more in 2014 compared to 2013.

Kaspersky Labs' Global Research and Analysis Team [55] observe the Equation Drug Trojan by the Equation Group. This malware copies information remotely and customized attacks for each of its victims. Trojan horse viruses are still being distributed through unsolicited emails today.

Pillai describes this malware as a cheap and easily distributed program that can take remote control of a computer. Cyber criminals use this virus as a means to illegally transfer money to overseas account after they obtain banking information from victims.

Russell examines a report that the Japanese government being hacked by a Chinese Trojan horse attack. This was discovered after a politician opened an email attachment. It is not clear what information was compromised. Maj Gen Shaw, who heads up the British Ministry of Defence's cyber programme, told the Daily Telegraph that "the biggest threat to the country by cyber is not military, it is economic". At this point in 2011, Asia had a reported 117 government websites that had been hit by Trojan viruses.

TYPES OF CYBERSECURITY

1. Network Security

Focuses on securing computer networks from unauthorized access, data breaches, and other network-based threats. It involves technologies such as **Firewalls**, **Intrusion detection systems** (IDS), **Virtual private networks** (VPNs), and **Network segmentation**.

- Guard your internal network against outside threats with increased network security.
- Sometimes we used to utilize free Wi-Fi in public areas such as cafes, Malls, etc. With this activity, 3rd Party starts tracking your Phone over the internet. If you are using any payment gateway, then your bank account can be Empty.
- So, avoid using Free Network because Free Network Doesn't support Securities.

2. Application Security

Concerned with securing software applications and preventing vulnerabilities that could be exploited by attackers. It involves secure coding practices, regular software updates and patches, and application-level firewalls.

- Most of the Apps that we use on our cell phones are Secured and work under the rules and regulations of the Google Play Store.
- There are 3.553 million applications in Google Play, Apple App Store has 1.642 million, and Amazon App Store has 483 million available for users to download. When we have other choices, this does not mean that all apps are safe.
- Many of the apps pretend to be safe, but after taking all information from us, the app shares the user information with the 3rd-party.
- The app must be installed from a trustworthy platform, not from some 3rd party website in the form of an APK (Android Application Package).

3. Information or Data Security

Focuses on protecting sensitive information from unauthorized access, disclosure, alteration, or destruction. It includes Encryption, Access controls, Data classification, and Data loss prevention (DLP) measures.

- Incident response refers to the process of detecting, analyzing, and responding to security incidents promptly.
- Promoting security awareness among users is essential for maintaining information security. It involves educating individuals about common security risks, best practices for handling sensitive information, and how to identify and respond to potential threats like phishing attacks or social engineering attempts.
- Encryption is the process of converting information into an unreadable format (ciphertext) to protect it from unauthorized access.

4. Cloud Security

It involves securing data, applications, and infrastructure hosted on cloud platforms, and ensuring appropriate access controls, data protection, and compliance. It uses various cloud service providers such as **AWS**, **Azure**, **Google Cloud**, etc., to ensure security against multiple threats.

- Cloud-based data storage has become a popular option over the last decade. It enhances privacy and saves data on the cloud, making it accessible from any device with proper authentication.
- These platforms are free to some extent if we want to save more data than we have to pay.
- AWS is also a new Technique that helps to run your business over the internet and provides security to your data

5. Mobile Security

It involves securing the organizational and personal data stored on mobile devices such as cell phones, tablets, and other similar devices against various malicious threats. These threats are Unauthorized access, Device loss or Theft, Malware, etc.

- Mobile is a very common device for day-to-day work. Everything we access and do is from a mobile phone. Ex- Online class, Personal Calls, Online Banking, UPI Payments, etc.
- Regularly backing up mobile device data is important to prevent data loss in case of theft, damage, or device failure.
- Mobile devices often connect to various networks, including public Wi-Fi, which can pose security risks. It is important to use secure networks whenever possible, such as encrypted Wi-Fi networks or cellular data connections.

6. Endpoint Security

Refers to securing individual devices such as computers, laptops, smartphones, and IoT devices. It includes antivirus software, intrusion prevention systems (IPS), device encryption, and regular software updates.

- Antivirus and Anti-malware software that scans and detects malicious software, such as Viruses, Worms, Trojans, and Ransomware. These tools identify and eliminate or quarantine malicious files, protecting the endpoint and the network from potential harm.
- Firewalls are essential components of endpoint security. They monitor and control incoming and outgoing network traffic, filtering out potentially malicious data packets.
- Keeping software and operating systems up to date with the latest security patches and updates is crucial for endpoint security.

6. Critical Infrastructure Security

- All of the physical and virtual resources, systems, and networks that are necessary for a society’s economics, security, or any combination of the above to run smoothly are referred to as critical infrastructure. Food and agricultural industries, as well as transportation systems, comprise critical infrastructure.
- The infrastructure that is considered important might vary depending on a country’s particular demands, resources, and level of development, even though crucial infrastructure is comparable across all nations due to basic living requirements.
- Industrial control systems (ICS), such as supervisory control and data acquisition (SCADA) systems, which are used to automate industrial operations in critical infrastructure industries, are frequently included in critical infrastructure. SCADA and other industrial control system attacks are very concerning. They can seriously undermine critical infrastructure, including transportation, the supply of oil and gas, electrical grids, water distribution, and wastewater collection.
- Due to the links and interdependence between infrastructure systems and sectors, the failure or blackout of one or more functions could have an immediate, detrimental effect on several sectors.

7. Internet of Things (IoT) Security

- Devices frequently run on old software, leaving them vulnerable to recently identified security vulnerabilities. This is generally the result of connectivity problems or the requirement for end users to manually download updates from a C&C center.
- Manufacturers frequently ship Internet of Things (IoT) devices (such as home routers) with easily crackable passwords, which may have been left in place by suppliers and end users. These devices are easy targets for attackers using automated scripts for mass exploitation when they are left exposed to remote access.
- APIs are frequently the subject of threats such as Man in the Middle (MITM), code injections (such as SQLI), and distributed denial of service (DDoS) attacks since they serve as a gateway to a C&C center. You can read more about the effects of attacks that target APIs here.

THE CYBER SECURITY PRINCIPLES

The purpose of the cyber security principles is to provide strategic guidance on how an organisation can protect their information technology and operational technology systems, applications and data from cyber threats. These cyber security principles are grouped into five functions:

- **GOVERN:** Develop a strong cyber security culture.
- **IDENTIFY:** Identify assets and associated security risks.
- **PROTECT:** Implement controls to manage security risks.
- **DETECT:** Detect and analyse cyber security events to identify cyber security incidents.
- **RESPOND**: Respond to and recover from cyber security incidents.

GOVERN PRINCIPLES

The govern principles are:

- **GOVERN-1:** A Chief Information Security Officer provides leadership and oversight of cyber security.
- GOVERN-2: Security risk management activities for systems, applications and data are embedded into organisational risk management frameworks.
- **GOVERN-3:** Security risks for systems, applications and data are accepted before they are authorised for use and continuously throughout their operational life.

IDENTIFY PRINCIPLES

The identify principles are:

- **IDENTIFY-1:** The business criticality of systems, applications and data is determined and documented.
- **IDENTIFY-2:** The confidentiality, integrity and availability requirements for systems, applications and data are determined and documented.
- **IDENTIFY-3:** Security risks for systems, applications and data are identified and documented.

PROTECT PRINCIPLES

The protect principles are:

- **PROTECT-1:** Systems and applications are designed, deployed, maintained and decommissioned according to their business criticality and their confidentiality, integrity and availability requirements.
- **PROTECT-2:** Systems and applications are delivered and supported by trusted suppliers.
- **PROTECT-3:** Systems and applications are designed and configured to reduce their attack surface.
- **PROTECT-4:** Systems, applications and data are administered in a secure and accountable manner.
- **PROTECT-5:** Vulnerabilities in systems and applications are identified and mitigated in a timely manner.
- **PROTECT-6:** Only trusted and supported operating systems, applications and code can execute on systems.
- **PROTECT-7:** Data is encrypted at rest and in transit between different systems.
- **PROTECT-8**: Data communicated between different systems is controlled and inspectable.
- **PROTECT-9:** Applications, settings and data are backed up in a secure and proven manner on a regular basis.
- **PROTECT-10:** Only trusted and vetted personnel are granted access to systems, applications and data.
- **PROTECT-11:** Personnel are granted the minimum access to systems, applications and data required to undertake their duties.
- **PROTECT-12:** Robust and secure identity and access management is used to control access to systems, applications and data.
- **PROTECT-13:** Personnel are provided with ongoing cyber security awareness training.
- **PROTECT-14:** Physical access to systems, supporting infrastructure and facilities is restricted to authorised personnel.

DETECT PRINCIPLES

The detect principles are:

- **DETECT-1:** Event logs are collected and analysed in a timely manner to detect cyber security events.
- **DETECT-2:** Cyber security events are analysed in a timely manner to identify cyber security incidents.

RESPOND PRINCIPLES

The respond principles are:

- **RESPOND-1:** Cyber security incidents are reported internally and externally to relevant bodies and stakeholders in a timely manner.
- **RESPOND-2:** Cyber security incidents are analysed, contained, eradicated and recovered from in a timely manner.
- **RESPOND-3:** Incident response, business continuity and disaster recovery plans support the recovery of normal business operations during and following cyber security incidents.

MATURITY MODELLING

When implementing the cyber security principles, an organisation can use the following maturity model to assess the implementation of individual principles, individual functions or the cyber security principles as a whole. The five levels of the maturity model are:

- **Incomplete:** The cyber security principles are partially implemented or not implemented.
- **Initial:** The cyber security principles are implemented, but in a poor or ad hoc manner.
- **Developing:** The cyber security principles are sufficiently implemented, but on a project-by-project basis.
- **Managing:** The cyber security principles are established as standard business practices and robustly implemented throughout the organisation.
- **Optimising**: A deliberate focus on optimisation and continual improvement exists for the implementation of the cyber security principles throughout the organisation.

COMMON TYPES OF CYBERATTACKS

1. Malware

Cyberattackers use harmful software such as spyware, viruses, ransomware, and worms known as malware to access your system's data. When you click on a malicious attachment or link, the malware can install itself and become active on your device.

2. Phishing

Phishing attacks rely on communication methods like email to convince you to open the message and follow the instructions inside. If you follow the attackers' instructions, they gain access to personal data, such as credit cards, and can install malware on your device.

3. Spoofing

Cyber attackers will sometimes imitate people or companies to trick you into giving up personal information. This can happen in different ways. A common spoofing strategy involves using a fake caller ID, where the person receiving the call doesn't see that the number is falsified. Other spoofing methods include subverting facial recognition systems, using a fake domain name, or creating a fake website.

4. Backdoor Trojan

Backdoor Trojan attacks involve malicious programs that can deceptively install malware or data and open up what's referred to as the "backdoor" to your computer system. When attackers gain access to the backdoor, they can hijack the device without it being known to the user.

5. Ransomware

Ransomware is malicious software that cyberattackers can install on your device, allowing them to block your access until you pay the attackers a ransom. However, paying the ransom doesn't guarantee the removal of the software, so experts often advise individuals not to pay the ransom if possible.

6. Password attacks

Password attacks can be as simple as someone correctly guessing your password or other methods such as keylogging, where attackers can monitor the information you type and then identify passwords. An attacker can also use the aforementioned phishing approach to masquerade as a trusted site and try to fool you into revealing your account credentials.

7. Internet of Things attack

Communication channels between connected IoT components can be susceptible to cyberattacks and the applications and software found on IoT devices. Since IoT devices are in connection with one another through the internet and may have limited security features, there is a larger attack surface that attackers can target.

8. Cryptojacking

Cryptojacking involves gaining unauthorized use of a computer system, usually through malware that allows the attacker to use the computer's resources for mining cryptocurrency. Mining cryptocurrency can come with significant operational costs, so cryptojacking provides attackers with a way to avoid these expenses.

9. Drive-by download

Drive-by download attacks occur when you download malicious code to your device through an app, website, or operating system with flawed security systems. This means you could do nothing wrong and still be a victim of a drive-by download since it can occur due to a lack of security measures on a site you believe to be safe.

10. Denial-of-service attack

A denial-of-service attack causes an entire device or operating system to shut down by overwhelming it with traffic, causing it to crash. Attackers don't often use this method to steal information. Instead, it costs the victim time and money to get their systems up and running again. Cybercriminals typically use this method when the target is a trade organization or government entity.

PREVENT OF CYBERATTACKS THREATS

Update your software.

Up-to-date software systems are more resilient than outdated versions, which may be prone to having weaknesses. Updates can correct any flaws and weaknesses in the software, so having the latest version is optimal. Additionally, consider keeping software systems updated by investing in a patch management system.

Install a firewall.

Firewalls are helpful in preventing a variety of attacks, such as backdoors and denial-of-service attacks. They work by controlling the network traffic moving through your system. A firewall will also stop any suspicious activity it deems potentially harmful to the computer.

Back up data.

When you back up data, you move it to a different, secure location for storage. This might involve using cloud storage or a physical device like a hard drive. In case of an attack, backing up your data allows you to recover any lost data.

Encrypt data.

Data encryption is a popular way to prevent cyberattacks, and it ensures data is only accessible to those who have the decryption key. To successfully attack encrypted data, attackers often have to rely on the brute force method of trying different keys until they can guess the right one, making breaking the encryption challenging.

Use strong passwords.

You should have strong passwords to prevent attacks and avoid using the same passwords for different accounts and systems. Using the same password repeatedly increases the risk of giving attackers access to all your information. Regularly updating your passwords and using passwords that combine special characters, upper and lowercase letters, and numbers can help protect your accounts.

ADVANTAGES OF CYBERSECURITY:

- Protection of Sensitive Data
- Business Continuity
- Compliance with Regulations
- Enhanced Customer Trust
- Competitive Benefit
- Early Detection and Response
- Intellectual Property Protection
- Reputation Protection
- Enhanced Collaboration
- Remote Work Security
- Improved Cyber Posture
- Removing Unwanted Programs
- Denying Unwanted Access
- Helps Educate the Workforce
- Easy Data Recovery

DISADVANTAGES OF CYBERSECURITY

- High Cost of Implementation
- Complex Management
- Potential False Sense of Security
- Compatibility Issues
- Inconvenience to Users

- ❖ Evolving Threat Landscape
- ❖ Human Error
- ❖ Limited Effectiveness Against Insider Threats
- ❖ Difficulties in Measuring ROI
- ❖ Balancing Security and Usability

3. CONCLUSION

In conclusion, cybersecurity issues and dangers are uniformly changeful and present serious risks to family, trades, and association. A complex and vital cyber countryside has existed presented on account of intensely evolution of science and the increasing relation of instruments and orders. As more schemes are enhanced, the attack surface expands, providing cybercriminals with more entrance points to exploit. This increases the risk of attacks on critical foundations, to a degree capacity grids, conveyance orders, and healthcare networks. Additionally, the shortage of skillful cybersecurity pros infuriates the challenges. There is an extreme demand for specialists who can efficiently discover, block, and put oneself in the place of other computer based threats. The shortage of these artists hampers organisations' strength to build healthy defences and react effectively to high-tech occurrence.To address these challenges and diminish warnings, organisations and individuals need to prioritise cybersecurity as a fundamental facet of their movements. The goal of computerised convicts is the computer world and the cyber protection breaches to a doubtful level.The science is hurtful and new belongings can seem more fearsome than they actually are. There is an increasing middle between cyber freedom and high-tech warnings. That will change the complete landscape of the computer network. A low fantasy is necessary to guarantee cyber safety, preventions and restore from cybercrimes and allure results. It grants permission to change the landscape of information technology.

4. REFERENCES

[1] A Sophos Article 04.12v1.dNA, eight trends changing network security by James Lyne.
[2] Cyber Security: Understanding Cyber Crimes- Sunit Belapure 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] International Journal of Scientific & Engineering Research, Volume 4, Issue 9,
[6] September-2013 Page nos.68 – 71 ISSN 2229-5518, “Study of Cloud Computing in HealthCare Industry “ by G.Nikhita Reddy, G.J.Ugander Reddy
[7] IEEE Security and Privacy Magazine – IEEECS “Safety Critical Systems – Next Generation “July/ Aug 2013.
[8] CIO Asia, September 3, H1 2013: Cyber security in malasia by Avanthi Kumar