International Journal of Scientific Research & Engineering Trends
Volume 10, Issue 5, Sept-Oct-2024, ISSN (Online): 2395-566X

Emerging Network Security Threats

Shashant Srivastava, Dr. Usha J
MCA Department
RV College of Engineering Bengaluru, India

Abstract- Over the past few decades, the rapid expansion of the Internet in India has brought significant challenges in ensuring network security. Network security encompasses the strategies and policies implemented by users to protect and oversee the network infrastructure from unauthorized access. This concept is crucial for both private and public networks in India, safeguarding communications and transactions. In recent years, India's networks have experienced substantial attacks from unauthorized entities. This paper examines the current network infrastructure and security policies in India, identifies the prevalent types of attacks, and proposes advanced technologies to enhance the robustness of India's network security framework

Index Terms- Network Security, Deep Learning, Blockchain, Hardware Authentication Method, Intrusion Detection System.

I. INTRODUCTION

Network security is defined as a set of activities encompassing both technical and non-technical measures aimed at protecting information, devices, computer resources, network resources, and other critical data from unauthorized access, modification, disruption, and disclosure.

The development of network security dates back to the 20th century, with the advent of technologies like antivirus software and firewalls in the 1990s, followed by Intrusion Detection Systems (IDS) and audio firewalls in the late 2000s.

Globally, the prevalence of network threats and security attacks has surged rapidly. Network systems have become prime targets for terrorists and hackers, leading to significant crises for nations and individuals alike.

These threats are categorized into unauthorized access, illegal use, data theft and destruction, phone and data line tapping, and virus dissemination. With the escalating issues in network security, a pressing question arises: can these threats be prevented, and are they hindering the development of the network? Networking is vital for countries, organizations, companies, and individuals, necessitating protection from unauthorized access, attacks, and destruction.

India faces significant threats due to the lack of network and cybersecurity infrastructure. Although the Indian government has initiated various programs and policies under the National e-Governance plan to update services available to citizens, these measures lack strong preventive strategies and are not sufficiently advanced. [1] In addition to this government, there is national level cyber- control and command mechanism to handle any cyber-related threats at the major and minor scale at any time in the digital expansion. Critical sectors such as Defense, Energy, Finance, Space, Telecommunication, Transport, and other public services heavily depends on the network to relay data, for communication purpose and for commercial transactions. So, these sectors have a large impact on using the Internet as a source of communication, and information.

According to Symantec Internet Security threat report, India ranks third in network attack after USA and China

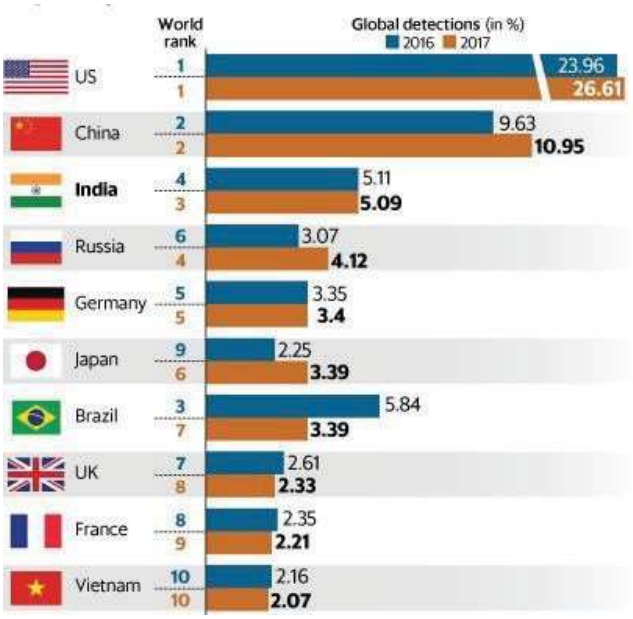

Fig.1. shows the list of top ten cyberthreat countries around the globe

© 2024 IJSRET

II. CURRENT SCENARIO OF NETWORK SECURITY INFRASTRUCTURE & POLICIES

Network attacks are increasingly prevalent and growing rapidly. India ranks second among countries recently targeted in their governmental and public sectors. The Indian government has recognized the need to protect its infrastructure and is addressing its flaws by updating existing technologies and services. Establishing a comprehensive cybersecurity framework is crucial to addressing cyber problems effectively over the long term. A major component of the national cybersecurity policy is to detect, deter, investigate and prosecute cyber-criminal activities. [1] By using this government can monitor and control the in/out defenses like national firewalls, proxies, network intrusion detection systems, intrusion prevention systems can be applied by using advanced technologies and process. [3] India needs amendment in laws and proper regulations on privacy and data protection. However, existing laws are already there for the company to protect its work. India currently has very few numbers of International internet Gateways and it is said that it will increase in near future.

Policies and Laws
The Cyber Security Laws and e-Security, as formulated by the Department of Electronics and Information Technology (Deity), Ministry of Communications and IT, Government of India, include:

Information Technology Act 2000
Defines Critical Information Infrastructure as a computer resource whose incapacitation or destruction would have a debilitating impact on national security, economy, public health, or safety.

Indian Copyright Act
States that any person who knowingly uses an illegal copy of a computer program shall be punishable. Computer programs are granted copyright protection but not patent protection.

Indian Penal Code
Section 406 addresses punishment for criminal breach of trust, and Section 420 deals with cheating and dishonestly inducing delivery of property.

National Cyber Security Policy — 2013
A policy framework by the Department of Electronics and Information Technology (Deity) aimed at protecting public and private infrastructure from cyber-attacks.

12th Five-Year Plan in the Information Technology Sector
This plan focuses on six key areas: enabling legal framework; security policy, compliance, and assurance; security research and development (R&D); security incident early warning and response; security awareness, skill development, and collaboration.

Departments [6]
The government of India has formed the various department for protection and prevention of Cyber threats in India. These departments listed below create cyber-security infrastructure and follow protocols.

National Cyber Command and Control Center (NCCC)l: It consists of an "NCCC committee" and a team of executive "NCCC cyber experts" along with members from NSCS, CIIP, CERT-IN, NIXI, DOT and head of the "NCCC cyber experts". Decisions are made by the team on control policies implementation at the PCC Boxes such that National e-sovereignty, national cyber interests, and the National CI/CIIs can be protected. Their job is it to suggest changes by adding, removing, modifying or reviewing the control policies. [1]

Monitor the performance of the PCC Boxes round-the- clock along with does a tactical and strategic analysis of national-Level cyber threats, attacks, and vulnerabilities to understand the potential consequences National Security Council Secretariat (NSCS): NSCS [6] department handle problems related to political, economic, energy and strategic security concerns of India. It is also a responsibility as secretariat to the NIB (National Information Board).

Critical Information and Infrastructure Protection (CIIP)
Provides access to public-private sources in India to focus on risk management, incident response and minimizing damage and along with recovery time to get a rapid or fast response to network crash or security breach. Provides with information about potential threats and vulnerabilities to take prevention and prepare with precautions measure, Conducts risk management evaluation and research assessment of threats and vulnerabilities to CII's.

Computer Emergency Response Team-India (CERT-IN)
Mission is "to enhance the security of India's Communications and Information Infrastructure through proactive action and effective collaboration". Alerts and monitors attacks at the public and private sector. It mostly manages Indian cyberspace and coordinates alerts and warning for India. It keeps check on Public, private, academia, Internet service provider and all information technology sources and products in the country

Department of Telecommunications (DoT)
Coordination of ISP's and all service providers in the country are to collaborate and work along with this department to provide the best support and guidelines. Due to these providers of all kind can ensure that their services as are uninterrupted and there are no physical attacks leading to data or information attacks.

© 2024 IJSRET

National Internet Exchange of India (NIXI)
Setup by DIT to maintain Internet Traffic across all services in India. Multilevel and multilayer cybersecurity infrastructure is required and is being planned to set up by the government. The national Internet traffic exchanges with the International Internet Gateways. CERT-IN, NIXI, DIT, CIIP, and NSCS acts as another layer of security as blocking objectionable content, domain control, cyber policies and laws creation and execution, cyber control, and cybersecurity research etc. [1]

III. TYPES OF ATTACKS IN NETWORK INFRASTRUCTURE

Major threats and attacks to network infrastructure can be classified into following types

- Passive attacks
- Active attacks
- Distributed attacks
- Insider attacks
- Close attacks. [10]

1. Passive Attack
In this attack, the attacker observes the data which is sent between the transmitter and receiver. The data can be a username, passwords or any other confidential messages. Passive attacks reveal the information of data files to the attacker without the information of the user [11]. Passive attacks use information of the system but don't affect the resources of the system. This attack has various types such as traffic analysis, monitoring of unprotected communications and capturing of passwords.

2. Active Attacks
In active attacks, the attacker exploits vulnerabilities in the system using malicious code to compromise and steal information. Once the security features are breached, the attacker can manipulate or transmit data as desired. These attacks often lead to system malfunctions, restrict user access to information, cause Denial of Service (DoS), and result in the disclosure of data files.

3. Distributed Attacks
Distributed attacks involve injecting malicious code into a system's software components to gain unauthorized access to its resources. The organization may remain unaware of the attack, leading to the distribution of compromised software to other users. This can result in the exposure of confidential information belonging to the organization or other institutions.

4. Insider Attacks
Insider attacks are carried out by individuals within an organization who have intimate knowledge of its infrastructure and policies. These insiders can easily access and disclose sensitive information about the system. Insider attacks are challenging to detect because network security policies are primarily focused on external threats.

5. Close-In Attacks
Close-in attacks involve attackers physically approaching network components, data, and systems to gather detailed information. By getting closer, attackers can alter information, restrict user access, and delete significant amounts of data.

IV. KEY TECHNOLOGIES USED FOR NETWORK SECURITY IN INDIA

The key technologies which India uses for providing network security are explained in this section

Firewalls
Firewalls, which can be hardware or software-based, are integral components of network infrastructure. They enforce organizational policies and permit access to selected network resources. Firewalls can be likened to a door lock in physical security, as they restrict access to only authorized users within the organization. They create a protective barrier between the network and external resources. When external network resources seek to access a specific organization's network, firewalls replicate the network at the entry point, ensuring that information is received promptly by the requesting network resources.

IDS (Intrusion Detection System): Intrusion Detection System is a [3] unique method to protect the network from any attacks. IDS come in hardware as well as software devices which are used to detect any attack. IDS keep an eye on the connection of the network to investigate whether an attack has been launched or not. There are some IDS products which are used to monitor and alert the system for any attack whereas other try to monitor as well as block it.

The most preferred example of IDS is an antivirus software product, anti-virus software systems have been used to detect any virus attacks and tries to block it. Use of IDS system is growing rapidly in both government and non- government organizations of India.

Anti-Malware Software: Anti-malware software is designed to detect and address various types of malware within a network. When malware is present, this software performs a scanning process to identify and neutralize it, preventing further damage to the network. Given the high volume of malware attacks faced by India, anti-malware software is a critical and widely used technology for network security in the country [3].

Data Encryption Technology: Data encryption technology is used for protecting data, files, password or any other

© 2024 IJSRET

confidential information. The methods used in data encryption technology are linked

V. DISADVANTAGES OF EXISTING TECHNOLOGIES USED FOR NETWORK SECURITY

The existing technologies used for network security in India has certain disadvantages as India has seen a success rate in the network attacks in the past few years due to certain disadvantages of the existing technologies. In this section, the disadvantages of the existing technologies like Firewalls, IDS (Intrusion Detection System), Anti-malware software and Data encryption technique has been explained. Firewalls: Firewalls which are a key tool for network security in India cannot protect the network infrastructure of India from virus threats as it is unable to scan each packet which contains viruses, also firewalls are designed for protecting the network from outside attacks but it cannot protect the network when any inside user attacks the network. [16]

1. Intrusion Detection System (IDS)

The Intrusion Detection System, used to alert the network to potential attacks, also has its drawbacks. One major issue is the reliance on source addresses; IDS works by analyzing network addresses sent as IP packets to the server networks. If a fake address is sent, it can cause the IDS to malfunction.

Another significant disadvantage is the problem of false alarms. IDS systems monitor network activity for behaviors that exceed normal operations, which can lead to numerous false alarms, especially in networks with high user activity. The likelihood of false alarms increases with the number of users on the network.

2. Anti-malware Software

The major disadvantages of anti- malware software is that it consumes much processing power of the systems and takes a lot more time for scanning the systems which give attackers enough time to launch another attack on the system, apart from this disadvantage it constantly needs upgrades it leads files to get blocked or deleted from the system.

Data Encryption Technology: Data encryption is a vital technology for securing data, but it comes with certain disadvantages. One major issue is the management of encryption keys; each piece of data is assigned a unique key, making it challenging to keep track of all the keys. Losing a specific key results in the loss of access to that data. Another significant drawback is the compatibility issue; integrating data encryption technology with existing applications can be complex, which can impact the daily operations of systems. [18]

VI. RECOMMENDATIONS FOR INFRASTRUCTURE & POLICIES

1. Proposed amendments to the IT Act

- **Section 43A: Liability of Companies:** Companies are responsible for maintaining their network procedures and implementing reasonable security practices.
- **Data Categorization:** Companies should define and differentiate between sensitive personal data or information and publicly accessible data.
- **Professional Bodies and Associations:** Recognize and incorporate the role of professional bodies and associations in cybersecurity.
- **Section 66:** Provides a more specific definition of data crimes.
- **Government Authorities:** Empower government authorities in cybersecurity to directly decrypt or access data to ensure the privacy protection of Indian citizens.
- **Investigation Procedures:** Strengthen investigation procedures to allow authorities to access data essential for investigations.
- **Technology Neutrality:** Introduce changes in definitions and technology neutrality at an intermediary level and consider implementing a system for collecting electronic signatures

2. Required advancement in Infrastructure and Technology

The policies and strategies of NCIIPC facilitate access to various technologies within India's information systems. All sectors related to information heavily rely on Critical Information Infrastructures (CIIs). The implementation of CII protection involves an analytical approach that starts with technical specifications and encompasses systems, actors, threats, vulnerabilities, consequences, and countermeasures. In addressing vulnerabilities, flaws, loopholes, or backdoors exploited by attackers to manipulate or control the system are considered.

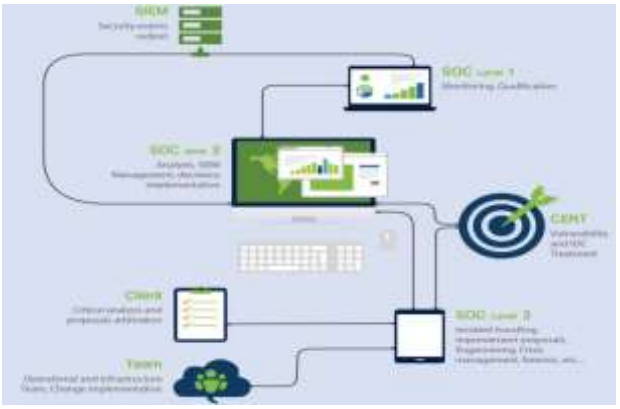

Fig. 2: Shows the infrastructure for protection at different levels

© 2024 IJSRET

The National Critical Information Infrastructure Protection Centre (NCIIPC) oversees policy and strategy related to access technologies and shared information systems in India. Critical Information Infrastructures (CIIs) are interconnected, interdependent, complex, and distributed across various geographical locations. Threats to CIIs, including terrorist attacks, organized crime, espionage, and malicious cyber activities, are increasing aggressively. The Government of India has designated NCIIPC as the national nodal agency under Section 70A (1) of the Information Technology (Amendment) Act 2008, responsible for implementing all measures, including research and development, to protect CIIs in India. [2]

3. The Emerging Technologies Which India Should Adopt for the Network Security

As seen in the previous section there are many disadvantages of the existing technologies which are used for network security in India. To overcome the disadvantages, offer by the existing technologies India must adopt these emerging technologies for the network security:

Hardware Authentication

The majority of network penetration happens in India because the password and username used by the users are very weak. This makes easy for the attackers to hack the data and steal the confidential data. This continuation of attack has increased pressure on the security experts to come up with a unique solution which can prevent this type of attack. The best way to stop this attack is by using hardware authentication method. Experts in the field of network security developed a solution for authenticating the username and password with the help generation of processors. Core V processor uses various hardware tools for user identification. Use of hardware authentication is also very important in the field of Internet of Things (IoT) where it ensures that the device has been connected to a particular network.

Cloud Technology

Cloud technology is the second most trending technology that enhances network security. It is widely used by both government and non-government enterprises for storing and sharing large amounts of information. Cloud technology increases network security approaches by enabling the migration of on-site data storage to the cloud. The network tools employed by cloud technology are virtual in nature compared to traditional forms. These tools include virtualized Intrusion Detection Systems (IDS), virtual firewalls, and virtualized system security.

Deep Learning

Deep learning combines machine learning and artificial intelligence, making it an excellent method for enhancing network security. The advantage of deep learning in network security is that when AI and machine learning systems are fed data on potential network threats, they can autonomously decide how to prevent attacks without human intervention. The use of machine learning allows for deep analysis of data entities.

Blockchain Technology

Many network attacks in India originate from within companies rather than from external sources. Blockchain technology provides a key method for enhancing network security by using a decentralized approach to data storage. Currently, data is stored in single files or systems, but blockchain technology stores data in an open-source manner, making it difficult for hackers to compromise the network. All network users will be aware of any attacks through the blockchain network. Blockchain security is a major contender for network security in large organizations, including government bodies and major private companies.

VII. CONCLUSION

The challenge of ensuring network security in India is significant, as the country continues to face threats from various unknown network sources. The current technologies employed for network security in India have several disadvantages that need to be addressed through the adoption of the latest technologies. Additionally, existing network security policies in India have certain flaws and require substantial amendments. In this paper, we recommend amendments and propose emerging technologies that India should integrate into its network infrastructure to better shield against continuous hacker attacks.

Acknowledgment

The authors would like to thank Next Tech Lab and RV College of Engineering for funding and providing resources for the research.

REFERENCES

1. Santosh Kumar Majhi “Cybersecurity issues and challenges” Journal of Global Research in Computer Science (JGRCS) vol. 6, no. 1, January 2015
2. Chaturvedi, Manmohan & Gupta & Bhattacharya, Jagjit. “Cyber Security infrastructure in India: a study”. January 2009
3. Guidelines for the protection of critical information infrastructure – National critical information infrastructure protection center (Government of India), 2018
4. Nandkumar Saravade “Cybersecurity initiatives in cybersecurity initiatives in India” (NASSCOM), 2007
5. Ministry of electronics and information technology – Government of India (Digital India)

© 2024 IJSRET

6. Donthula Ravi Kumar "Indian perimeter cybersecurity: cybersecurity policy and implementation" (2016-IJARCS) vol. 6, issue 7, July 2016
7. Vivek Gurung, "the national cybersecurity policy-2013 of India ", cyber Kendra, latest hacking news and tech news, Jul 2013.
8. Indian computer emergency response team, Department of Electronics & information technology, Ministry of communications & information technology, http://www.cert-in.org.in
9. Department of telecommunications (dot), Ministry of communications & information technology, http://www.dot.gov.in
10. National internet exchange of India (NIXI), http://nixi.in.
11. "Guidelines for the protection of national critical information infrastructure"– version 1.0 2013.
12. Barshitha B, N Ramesh "A survey of different types of network security threats and its countermeasures" International journal of advanced computational engineering and networking volume- 1, issue- 6, Aug-2013.
13. Monali S. Gaigole, prof. M. A. Kalyankar "The study of network security with its penetrating attacks and possible security mechanisms" International journal of computer science and mobile computing vol. 4, issue. 5, May 2015.
14. Jian He "The research of computer network security and protection strategy" American Institute of physics Doi: 10.1063/1.4982538.
15. Rahul Pareek "Network security: an approach towards secure computing" Journal of global research in computer science vol. 2, no. 7, July 2011
16. Dr. Ajit Singh, Madhu Pahal, and Neeraj Goyal "A review paper on firewall" International journal for research in applied science and engineering technology.
17. Imtithal a. Saeed, Ali Selamat, and Ali M. A. Abuagoub "Survey on malware and malware detection systems," international journal of computer applications, vol. 67–no.16, April 2013.
18. Nilotpal Chakraborty "Intrusion detection system and intrusion prevention system: a comparative study" International Journal of computing and business research, vol. 4, Issue 2 may 2013.
19. Md Asif Mushtaque "Comparative analysis on different parameters of encryption algorithms for information security" International journal of computer sciences and engineering vol.2, issue-4.

© 2024 IJSRET