Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 9, No.1, September : 2024

CYBER SECURITY: A NEED OF ERA

Ms. Amrit Kaur, Ms. Pooja, Assistant Professor, Dept. of Computer Science and Applications, UICA&IS, Sant Baba Bhag Singh University.
Er. Harjit Kaur, Assistant Professor, Dept. of Computer Science and Engineering, UIET, Sant Baba Bhag Singh University.

ABSTRACT
Security is the key concern in every field. As in modern world, cyber plays an important role. Human beings become a slave of cyber for its daily work. So, cyber security is the need of modern society because all important information and files are transferred on the Internet. So, in order to protect these files, a security mechanism is needed. Cyber Security provides a security to the data that is transferred online in cyber space. Now-a-days sensitive data is breached by various attackers. Hence, this paper highlights the way of breaching the security of cyber with some precaution measures. Moreover, it also illustrates various ethics that are followed in cyber.
Keywords: cyber, security, ethics, breaching, cyber security

I. Introduction

In this hustle and bustle environment, everybody wants to use alternate way of internet to do their tasks. So, it's crucial to provide security to exchange of information on the Internet. This could be achieved with the help of cyber security that aims at providing security to computers, electronic systems, servers, networks, and mobile devices from the various types of malicious attacks. This term may be used in lots of contexts, which may vary from mobile computing to business, and can further be divided into various classes. [1]

· The first class is Network security. It is the way of hiding a network from the intruders/hacker, whether it may target an opportunistic malware or attackers.

· The second category is Application security that focuses on keeping an eye on devices and software to check whether they are free of threats. A well-maintained application may gain access to the data it was designed to protect. Good security starts at the design stage, long before any program or device is used.

· The third class in Information security which aims at protecting the privacy and integrity of data which may be in transit or storage phase.

· The fourth one is Operational security that indulge the decisions and processes for protecting and handling the assets of data. All the procedures and permissions that users generally have while accessing the network will be stored and shared by this.

· The fifth is Disaster recovery with business continuity. It aims at defining what should be done by an organization that causes loss of data and operations and how they will deal with their cyber security. This policy demonstrates an organization to restore their information or operations before any disaster. However, the plan of business continuity lack behind due to lack of certain resources.

· The sixth and the last one is the end user that is people. It is the complex and complicated factor for cyber security because anyone can inject the virus in the computer system without knowing the good practices of security. Some of the practices with which viruses can easily enter the system are suspicious email attachments, attachments of USB with the system.

II. Types of Threats

The three-fold threats that are countered by cyber-security are as follows: [6]

1. Cybercrime: It is the type of threat which includes a single intruder or the groups of the individual that targets the systems for to gain financial benefit from the host or cause disruption to the system.
2. Cyber-attack: It aims at getting information about the political activities of the country.
3. Cyberterrorism: It aims at using electronic media to create fear or panic among the people.

In order to create threats to the system, the main question arises how the intruder takes the control of the system? The following are the answer for the question. In order the intruder uses the following techniques to take control of the system and threaten the security of the cyber.

i. Malware: In simple term it is the malicious software. Malware, one of the mostly used threats not unusual on-line threats, is software program created by using cybercriminals or hackers to disrupt or harm valid users' computers. Malware is frequently delivered via illegal emails or legitimate-looking downloads and can be used by cybercriminals to make money or purpose cyberattacks.

There are numerous forms of malware, which includes:

- Virus: A self-reworking software that attaches with the clean records and spreads for the duration of the pc, infecting it with awful information.
- Trojans: It is the type of the malware in which the malicious software looks exactly legitimate software. It is the trick of the cybercrimes to upload the Trojans smartly into the computer and collect data or cause damage to the system.
- Spyware: it is the threat in which the intruder secretly keeps an eye on which the user does on his/her system. After that intruder uses that information to harm the user. For instance, intruder secretly steals the information of the credit card or debit card while shopping online and then uses the information to steal money of the user.
- Ransomware: It is an attack in which attacker locks the important files of the user and demands for the ransom. If it will not be paid then threats to delete the files or information.
- Adware: It is an advertising software that can be used in spreading malware.
- Botnets: It is the type of malware in which infected computers perform the various tasks without the permission of user.

ii. SQL injection

It is a type of attack that is used to attack the database. In SQL injection, the attacker takes the control of the database and then steal the required information from the database. The intruders try to insert the infected code by using SQL (Structured Query Language) statements and gets the access to the database in which the sensitive information is present.

iii. Phishing

It is the type of the attack in which attacker attack the user via email. The attacker sends the email to the user in such a way that it looks that the email is from legitimate company and ask for the sensitive information from the user.

iv. Man-in-the-middle attack

It is the attack in which the intruder or hacker disturbs the communication taken place between two persons so that the intruder steals their information.

v. Denial-of-service attack

It is the process in which intruder pretends the user that the network or machine which the user wants to use is not available to use. It mainly takes place by flooding the packets on the machine and makes the machine overloaded so that the machine does not fulfil the request of the user.

vi. Latest cyber threats

There are some of the threats are commonly found in the modern world. Some of them are as follows:

- Dridex malware

These diabolical plans have affected citizens, governments, infrastructure, and the global economy. Since 2014, it has been affecting victims by infecting computers via phishing emails or existing malware. The ability to steal passwords, banking information and personal information used in fraud results in hundreds of millions of dollars in financial losses. Patches are applied, antivirus software is turned on and up to date, and data is backed up.

- Romance scams

The FBI issued a cautionary notice to Americans, advising them to stay vigilant against confidence scams orchestrated by cybercriminals via dating platforms, chat rooms, and mobile applications in February, 2020. Exploiting the vulnerability of those in search of companionship, perpetrators deceive

individuals into divulging sensitive personal information. According to FBI data, romance-related cyber threats victimized 114 individuals in New Mexico alone in 2019, resulting in financial losses totaling $1.6 million.

- Emotet malware

Towards the end of 2019, the Australian Cyber Security Centre (ACSC) issued a cautionary alert to domestic entities regarding a pervasive global cyber menace stemming from Emotet malware. Emotet, a highly sophisticated trojan, possesses the capability to pilfer data and deploy additional malware. Its success hinges on exploiting simple passwords, serving as a stark reminder of the criticality of crafting robust passwords to fortify defenses against cyber threats.

- End-user protection

Endpoint security, a critical component of cybersecurity, safeguards against the inadvertent introduction of malware or other cyber threats by end-users onto their desktops, laptops, or mobile devices. So, how exactly do cybersecurity measures shield end-users and systems? Firstly, cryptographic protocols are utilized to encrypt emails, files, and other sensitive data, not only securing information during transmission but also thwarting potential loss or theft.

Furthermore, end-user security software conducts thorough scans of computers to identify and quarantine pieces of malicious code, subsequently eliminating them from the system. These security programs are adept at detecting and eradicating malicious code concealed within the Master Boot Record (MBR), and they are equipped to encrypt or erase data from the computer's hard drive if necessary.

Moreover, electronic security protocols prioritize real-time malware detection, employing heuristic and behavioral analyses to monitor program behavior and code, thereby defending against viruses or Trojans that alter their appearance with each execution (such as polymorphic and metamorphic malware). Security software isolates potentially malicious programs within a virtual environment separate from the user's network, enabling analysis of their behavior to enhance detection of new infections.

As cybersecurity professionals uncover new threats and innovative ways to combat them, security programs continually evolve with new defensive mechanisms. Effective utilization of end-user security software necessitates educating employees on its proper use. Crucially, regular updates and maintenance ensure that the software remains equipped to safeguard users against the latest cyber threats.

III. Measures

The following are the various guides for businesses and common individual that helps in protecting from intruder and provides security online to cyber space. [7]

Businesses must implement diverse cybersecurity protocols to safeguard their business data, financial transactions, and customer information in the online realm. These protocols should be designed to mitigate risks originating from multiple sources, such as internet-borne threats like spyware or malware, vulnerabilities arising from user-generated weaknesses like weak passwords or mishandled information, and flaws inherent in system or software architecture that can be exploited to compromise security measures. Key cybersecurity measures encompass a range of processes and tools that, when implemented together, establish a foundational level of security against prevalent IT risks.

a) Have strong passwords

Creating robust passwords is essential for maintaining strong online security. Ensure your password is challenging to decipher by incorporating a mix of uppercase and lowercase letters, numbers, and symbols. Aim for a length between eight and 12 characters, avoiding the inclusion of personal information, and regularly changing it. Refrain from using the same password across multiple accounts and consider implementing two-factor authentication for added protection. Establish a password policy within your business to encourage adherence to security best practices among staff. Explore various technological solutions, such as scheduled password resets, to enforce your password policy

effectively. For comprehensive guidance on password management, consult the National Cyber Security Centre's (NCSC) password protection guide and explore diverse password strategies to enhance your business's security posture.

b) Data and systems are controlled by providing access to user:

Ensure that individuals can only access data and services for which they have authorization. This can be achieved by:

- Physical access should be managed in computer networks and in premises.
- Restricting access to authorized users only.
- Implementing application controls to limit access to specific data or services.
- Regulating the copying and saving of data onto storage devices.
- Limiting the sending and receiving of certain types of email attachments.

Utilize modern operating systems and network software to facilitate these measures, but also manage user registration and authentication systems, such as passwords, to enhance security further. For further guidance, refer to the NCSC's introduction to identity and access management controls.

c) Putting up the firewall

Firewalls act as essential barriers between your computer and the internet, playing a crucial role in thwarting cyber threats such as viruses and malware from infiltrating your system. It's imperative to properly configure and consistently maintain firewall devices to ensure their efficacy. Regular updates of their software or firmware are vital to uphold optimal security standards. For deeper insights into the significance of firewalls in server security, delve into their role in safeguarding sensitive data and preventing unauthorized access to critical resources.

d) Use security software

Employ security software like anti-spyware, anti-malware, and anti-virus programs to detect and eliminate malicious code that may infiltrate your network. Refer to our comprehensive guidance to aid in detecting spam, malware, and virus attacks effectively.

e) Update systems and programs on regular basis

Updates are essential as they include critical security enhancements that safeguard against known bugs and vulnerabilities. Ensure that you regularly update your software and devices to thwart potential exploitation by cybercriminals.

f) Monitor for the intrusion

Incorporate intrusion detectors to oversee systems and detect any abnormal network behavior. When a detection system flags a potential security breach, it triggers an alarm, such as an email alert, tailored to the identified activity type. Explore further insights on cyber security breach detection for a comprehensive understanding.

g) Raise awareness

Ensure that your employees are aware of their responsibility in maintaining the security of your business. Provide them with thorough understanding of their roles, relevant policies, and procedures, and regularly conduct cyber security awareness and training sessions. Familiarize yourself with insider threats in cyber security for further insights.

Adhere to the best practices outlined in the government's Cyber Essentials scheme.

Utilize the National Cyber Security Centre's (NCSC) free Check your cyber security service to conduct simple online checks aimed at identifying common vulnerabilities in your public-facing IT infrastructure.

Additionally, take advantage of the NCSC's free Cyber Action Plan. By answering a few straightforward questions, you can receive a personalized action plan highlighting immediate steps you or your organization can take to fortify against cyber-attacks.

h) IDS (Intrusion Detection System)

An intrusion detection system (IDS) is a software designed to monitor network traffic for suspicious or malicious activity and promptly alert administrators upon detection. It continuously checks networks or systems for any signs of unauthorized activities or breaches of security policies. Incidents

are typically logged either centrally using a Security Information and Event Management (SIEM) system or reported directly to administrators. IDS functions by monitoring network or system behavior and safeguarding against unauthorized access, including potential threats from insiders. The primary objective of an intrusion detection system is to develop a predictive model, such as a classifier, capable of effectively differentiating between 'bad connections' and 'good connections'. In this, ‘bad connection is the attacker or intruder where as ‘good connection’ is the normal one which is done by legitimate user. [6]

The working of IDS is explained as follows:

• It monitors computer network traffic to identify potentially suspicious activity.
• It scrutinizes the data traversing the network, seeking out anomalies and irregular behavior.
• Comparing network activity against established rules and patterns, the IDS flags any instances that suggest a potential attack or intrusion.
• Upon detecting such activity, the IDS promptly notifies the system administrator through an alert.
• The system administrator investigates the alert and implements necessary measures to mitigate damage or prevent further intrusion.

The Figure 1 demonstrates the pictorial representation of Intrusion Detection System. In which, the host computer’s data enters into IDS where the data is monitors for the malicious activities. After that, the data enters into the firewall for filtering of the data. Then, the data is routed with the help of router towards the Internet. This figure describes the simple working of the IDS.

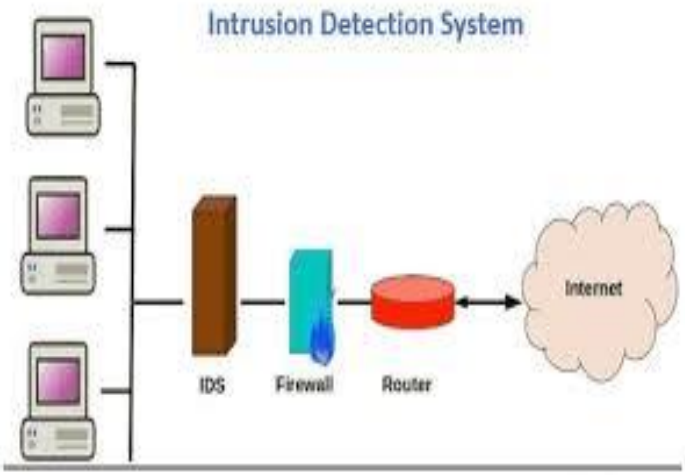

Figure 1: Intrusion Detection System

The IDS is further classified into 5 categories. [6] These are:

• Network Intrusion Detection System (NIDS): These are strategically positioned within a network to scrutinize traffic emanating from all connected devices. They conduct comprehensive monitoring of traffic across the entire subnet, comparing it against a database of recognized attack patterns. Upon detecting any malicious activity or anomalous behavior, NIDS promptly notifies the administrator, enabling timely response. For instance, placing a NIDS on the subnet housing firewalls allows for vigilance against potential attempts to breach the firewall's defenses.

• Host Intrusion Detection System (HIDS): It operate autonomously on individual hosts or devices within the network. These systems focus on scrutinizing both incoming and outgoing packets specific to the host they're installed on. They are designed to promptly notify the administrator upon detecting any indications of suspicious or malicious behavior. Additionally, HIDS periodically capture snapshots of the system's current files and compare them with previous snapshots. Any alterations or deletions to critical system files trigger an alert, prompting further investigation by the administrator. One common scenario for HIDS implementation is safeguarding mission-critical machines that are intended to maintain a consistent configuration.

- Protocol-based Intrusion Detection System (PIDS): It consists of a system or agent positioned at the forefront of a server, tasked with managing and interpreting the communication protocol between a user/device and the server. Its primary objective is to fortify web servers by continuously monitoring the HTTPS protocol stream alongside its associated HTTP protocol. Given that HTTPS traffic is encrypted, this system requires placement at the interface between users and the HTTPS, enabling it to analyze incoming traffic before it reaches the web presentation layer.
- Application Protocol-based Intrusion Detection System (APIDS): It is a system or agent typically situated within a cluster of servers. Its function involves detecting intrusions by continuously monitoring and analyzing communication occurring on application-specific protocols. For instance, APIDS might focus on scrutinizing the SQL protocol as it facilitates transactions between the middleware and the database within a web server environment.
- Hybrid Intrusion Detection System: It combines two or more approaches to intrusion detection. In this system, data from host agents or systems is integrated with network information to provide a comprehensive perspective of the network. This integrated approach enhances effectiveness compared to standalone intrusion detection systems. Prelude serves as an example of a Hybrid IDS.

The following Figure 2 illustrates the various types of IDS (Intrusion Detection System)

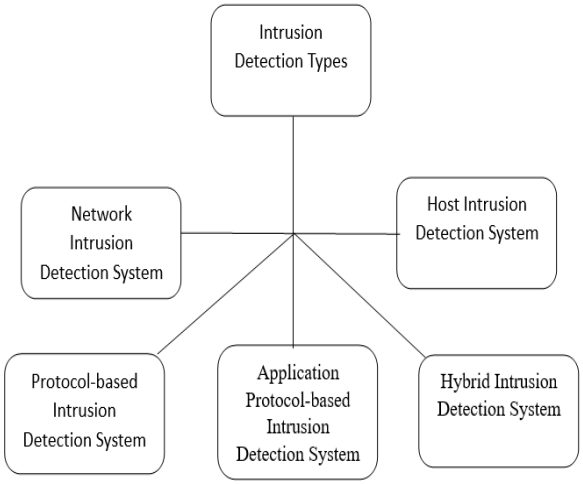

Figure 2: Types of Intrusion Detection System

IV. Cyber Ethics

The ethics in the cyber serve as the guiding principles for the ethical conduct in the online realm, essentially forming a moral compass for internet usage. Adhering to these principles greatly enhances the likelihood of utilizing the internet in a proper and safer manner. Below are several key cyber ethics to observe:

- Do use the Internet for communication and interaction: Platforms like email and instant messaging facilitate easy communication with friends, family, and colleagues worldwide, enabling the exchange of ideas and information across distances.
- Avoid cyberbullying: Refrain from engaging in behaviours such as name-calling, spreading lies, or sharing embarrassing content about others, as these actions can cause harm and distress.
- Respect intellectual property: Recognize the internet as a vast repository of information and ensure that its contents are used in a legal and ethical manner, respecting copyright laws and intellectual property rights.
- Maintain online integrity: Avoid unauthorized access to others' accounts and refrain from attempting to compromise their systems with malware. Similarly, safeguard personal information to prevent potential misuse and avoid impersonating others or creating fake accounts, which can lead to legal repercussions for both parties involved.

- Adhere to copyright laws: Respect the rights of content creators by only downloading games, videos, or other copyrighted material from legitimate sources with proper authorization.

By upholding these cyber ethics, individuals can contribute to a safer and more respectful online environment. Just as we learn proper rules and behaviour from an early age, applying these principles in cyberspace is essential for responsible internet usage.

V. Conclusion

The manuscript contains the general information about cyber security. It is the technique of securing various activities that are performed online. It also highlights various attacks that are performed on the online activities. Moreover, it demonstrates various methods with which someone can secure their activities on the cyber space.

It also provides information about the cyber ethics that are followed during online data transfer.

References

[1] IEEE Security and Privacy Magazine – IEEECS "Safety Critical Systems – Next Generation "July/ Aug 2013.

[2] International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013 Page nos.68 – 71 ISSN 2229-5518, "Study of Cloud Computing in HealthCare Industry " by G.Nikhita Reddy, G.J.Ugander Reddy.

[3] https://www.kaspersky.co.in/resource center/definitions/what-is-cyber-security.

[4] "A Study of Cyber Security Challenges and its Emergning Trends on Latest Technologies" by G.Nikhita Reddy, G.J.Ugander Reddy.

[5] https://www.geeksforgeeks.org/intrusion-detection-system-ids/

[6] Cyber Attack Trends Analysis Key Insights to Gear Up for in 2019. Available Online: http://www.snt.hr/boxcontent/ CheckPointSecurityReport2019_vol01.pdf.

[7] IEEE Security and Privacy Magazine – IEEECS "Safety Critical Systems – Next Generation "July/ Aug 2013.

[8] Cyber Security: Understanding Cyber Crimes- Sunit Belapure Nina Godbole.