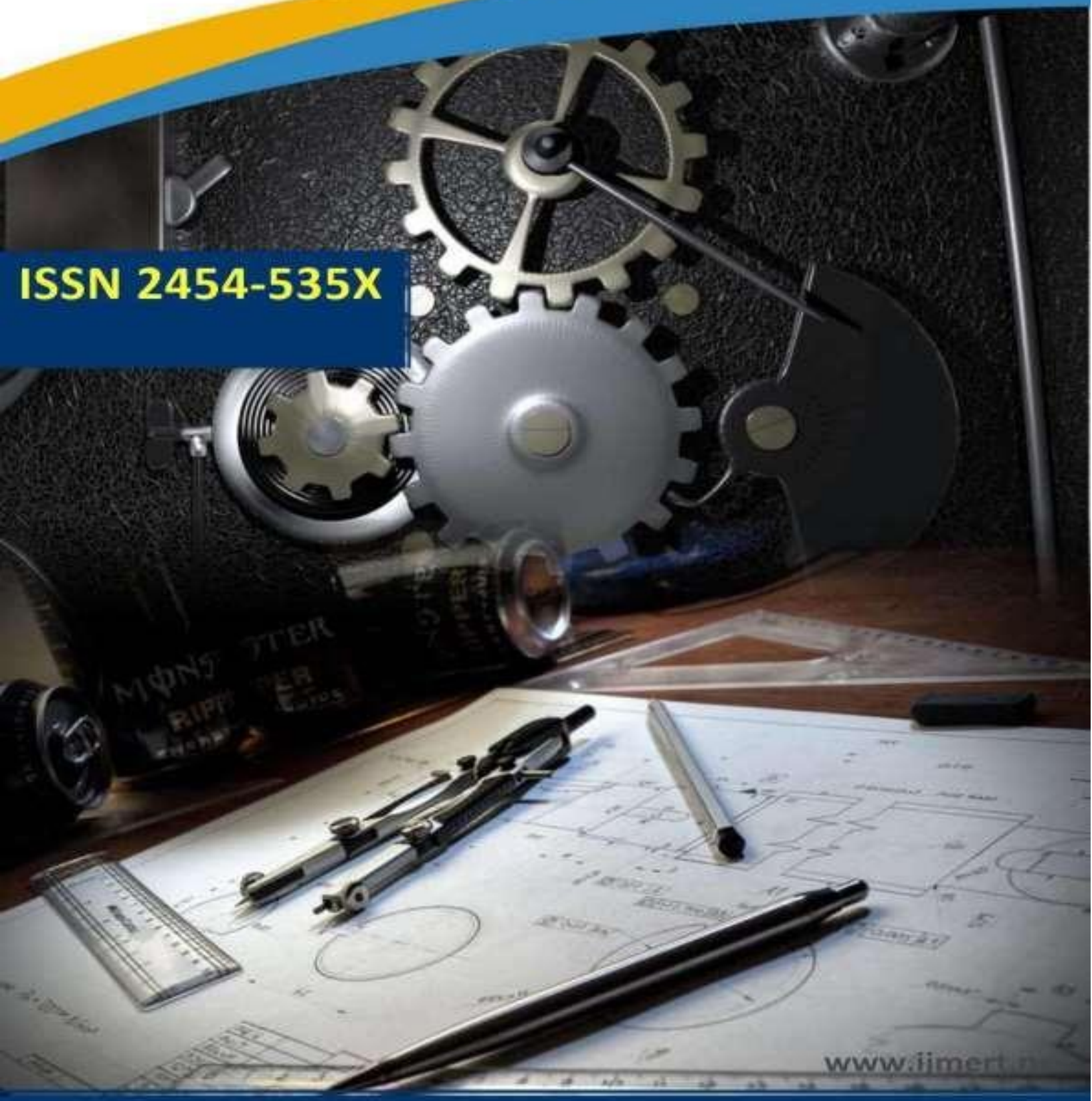
International Journal of Mechanical Engineering Research and Technology

ISSN 2454-535X



Email ID: info.ijmert@gmail.com or editor@ijmert.net

International Journal of Mechanical Engineering Research and Technology

ISSN 2454 – 535X www.ijmert.com
Vol. 16 Issue. 2, May 2024

What are Cyber-Threats, Cyber-Attacks and how to defend our Systems

Choppa Manikanta Kalyan M.Tech
Manikantacm016@gmail.com

ABSTRACT
Technology is altering our brains, and the generational divide between the "digital immigrants" and the "young natives" is widening, according to a study published on the UCLA website. (Gary Small, MD) Technology has grown in importance to the point that it dominates practically every aspect of modern life. This includes fields as diverse as medicine, education, employment, entertainment, and communication. Attacks directed at computer systems or hardware with the intent to do damage to individuals, businesses, or government agencies are sometimes referred to as cyber wars or cyber attacks.

INTRODUCTION

The History (Chapter 1)

Every aspect of our lives, from communication to shopping to employment, is now facilitated by technology.

appreciating the night. A data breach might have serious consequences for both our firm and the targeted one. Up to 40 million customers may have had their debit and credit card information compromised in a security breach at Target shops in the United States, according to a story published on December 20, 2013, by Megan Hazle. As stated by Hazle in 2013. On top of that, it is estimated that every American household has at least five internet-connected gadgets that transmit sensitive information like login credentials and bank account details. On top of that, an article by Mark Milian and Jordan Robertson was published on April 23, 2013, on the technology page of Bloomberg News. The report claims that China was responsible for as much as 41% of the world's computer-attack traffic in Q3 2012. That is according to (Milian & Robertson, 2013).

Because of their portability and the fact that many people keep sensitive information (such as bank account details, social security numbers, passwords, etc.) on their smartphones and tablets, these devices are increasingly vulnerable to cyberattacks. Nowadays, technology plays a significant role in almost every aspect of our personal lives. That is why it is crucial to bolster the security of the devices we use, establish rules and regulations to safeguard personal information, and combat cybercrime so that criminals can't damage innocent people online. Only then can we ensure that our nation's assets are safe from harm and attacks.

Cybersecurity is a new lexicon that unifies concepts like information security and computer security. All actions including threats, attacks, hacks, and the software used for security or attack will be referred to by this language. Our nation's federal government agencies and the National Initiative for Cyber Security Education (NICE) agree that there is a lack of uniformity in the definition and description of cyber security (NICE, 2012). The company's online operations are vulnerable to a wide variety of risks and assaults; for example, businesses dealing with financial transactions are particularly vulnerable to

International Journal of Mechanical Engineering Research and Technology

ISSN 2454 – 535X www.ijmert.com
Vol. 16 Issue. 2, May 2024

Virtual Privet Network (VPN) attacks, also known as Remote Access
Any kind of assault or threat directed at a computer over an internet-connected network is considered a cyber-attack. Any number of computers, online applications, or web servers might be the targets of the assault. A person, company, or government agency's system might be the subject of a variety of threats and assaults. Defining cyber-attacks, dangers, and cyber-crime using new terminology The purpose of this division is to resolve these matters in accordance with applicable laws and regulations.

The UN estimates that about six billion people throughout the globe use mobile phones. This makes it an attractive target for attackers looking to do damage, given the world has around 6 billion cell phone subscribers (U.N. Telecom Agency Report, 2012 ¶ 1). on the moveThere is a wide variety of devices available, each with its own unique brand and operating system.

While some manufacturers, like Apple, use iOS, others, like Samsung and HTC, use Android, while still others, like Nokia and Blackberry, use their own operating systems. People who hack do so for a variety of reasons; some do it for fun, while others are professionals with ties to terrorist groups, government organizations, or other groups with financial interests. A great opportunity for this hacker to indulge their hobby has presented itself, thanks to the abundance of mobile devices and desktop, laptop, and tablet computers. Cybercriminals will refer to any device—portable or desktop—connected to the internet and networks as a target in their quest to steal sensitive information or just make money. Today, technology permeates nearly every aspect of our personal lives. This highlights the critical importance of securing the devices we use, establishing laws and regulations to safeguard personal information, combating online crime, identifying and apprehending criminals, and protecting national assets from harm.

The many forms of cyber threats and assaults, as well as self-defense strategies, attack details, and methods for securing computers and mobile devices, will all be covered in this research.

Chapter 2: The Issue

People may save sensitive information on their own personal devices, such as laptops, desktops, tablets, and smartphones, and there are organizations online whose only purpose is to get sensitive information. These organizations are notorious for their hacking activities; they actively seek for ways to exploit system or network weaknesses in order to launch attacks. People are not the only ones these gangs target.
Businesses and public entities might be their targets. Damage to the company's reputation, integrity, and bottom line, as well as the likelihood of such losses occurring again, Businesses must learn the rules of standards and implement them to protect their networks and systems. Hence, the many potential dangers and assaults on the network, computers, and portable devices will be addressed in this plan. In addition, we will educate ourselves to learn more about Cyber Security and go over various methods to identify and safeguard the technologies we use.

The Purpose/Significant (Chapter 3)

Up to 40 million customers may have had their debit and credit card information compromised in a security breach at Target shops in the United States, according to a story published on December 20, 2013, by Megan Hazle. As stated by Hazle in 2013. On top of that, according to an It is estimated that the average American household has five or more internet-connected gadgets, all of which transmit sensitive information including login credentials and bank account details. Furthermore, on April 23, 2013, Mark Milian and Jordan Robertson of Bloomberg News published an item on their technology page asking if China was responsible for 41% of the world's computer-attack traffic in the fourth quarter of 2012. That is according to (Milian & Robertson, 2013). Smartphones and tablets are also vulnerable to hacking attempts. The fact that many

International Journal of Mechanical Engineering Research and Technology

ISSN 2454 – 535X www.ijmert.com
Vol. 16 Issue. 2, May 2024

individuals keep private information—including passwords, bank account details, and social security numbers—on their mobile devices makes them an attractive target for cybercriminals. The significance of understanding potential dangers, assaults, and ways to protect our systems is highlighted by this data. These dangers affect everyone using the internet, not just businesses.

Our safety is at stake if the research does not proceed. Insights on the assaults and methods for protecting sensitive information will be provided by this study. Education ranks high among the details that may aid in thwarting an assault individuals should be aware that they greatly increase their vulnerability to attacks and data theft by opening emails from unknown senders. Is anybody out there Anyone interested in cyber security may benefit from this study as it provides all the necessary information to understand how to protect one's computer or network. With regards to the methods used for system security.

The Vulnerabilities and Threats (Chapter 4)

Any weak spot in the operating system, the network, or the software that is in use poses a threat since it might be exploited in a cyberattack. The software and operating system of a computer will identify any potential threats to the machine or the data stored on it. Another element that affects and increases the danger is the user. Sometimes, the user may unknowingly approve of the attacker hacking the computer. In the absence of an antivirus or other malware detection,

Without software to regulate money flow, the machine is more vulnerable to attacks, thus it's important to employ antimalware software. The Emerging Cyber attacks 2012 study states that the most mobile threat vector was the most well-known cyber danger in 2012. This is due to the following reasons: mobile browsers provide a unique difficulty, mobile devices are not regularly patched and updated, and attacks targeting iOS and Android are increasing. A robust mobile security program that prioritizes encapsulation is essential, since mobile devices provide a new entry point for cybercriminals to target networks and mission-critical infrastructure. Pages 2, 3, and 4 of the 2012 publication by Ahamad et al. The number of people using mobile devices and tablets continues to rise, and by 2014, it could surpass the number of people using desktop PCs to access the internet (Ahamad, et al., 2012, p. 3) Because of this, we've seen a surge in the number of apps designed for tablets and smartphones; almost all of these

There may be a rise in online assaults targeting individuals using these apps, depending on the web browser (Ahamad, et al., 2012, p. 3). Web browsers may be problematic at times due to the fact that websites are often created with desktop PC screens in mind. As a result, users may encounter difficulty while trying to access certain pages. The Internet Control Systems Emergency Response Team (ICS-CERT) defines cyber risks as any effort to gain unauthorized access to a computer system or network, whether by an employee or an outsider to the company. Many different entities pose cyber risks, including hostile governments, terrorist organizations, angry

contractors, and malevolent outsiders. (Descriptions of Cyber Threat Environments). Cyber criminal syndicates, small-time crooks, hacktivists, the ever-increasing Web of compromises, botnets as a service, all-in-one malware, intellectual property theft and corporate espionage, and cyber warfare are among the most significant cyber risks that any computer user may face. (The Nine Most Dangerous Concepts in Cybersecurity Today) Emerging cyber threats ranked highest Priority one The United States intelligence community ranked cybercrime as the top global danger in 2013, followed by transnational organized crime and terrorism, WMD, space exploration, resource competitiveness, health and pandemic concerns, and mass atrocities. (Pellerin, 2013) page 3. All computer, network, and connection vulnerabilities are considered cyber threats.

International Journal of Mechanical Engineering Research and Technology

ISSN 2454 – 535X www.ijmert.com
Vol. 16 Issue. 2, May 2024

operating system and software currently in use. Because of their central location on the internet and the high volume of data stored there, information systems are particularly at risk from cyberattacks; consequently, it is imperative that these systems implement robust cyber defenses. Different kinds of security holes in computer systems and networks that may be exploited by malicious actors.

The Types of Attacks (Chapter 5)

Hackers targeting a web server online will also target the system's backups and databases, since these are its weakest points. The goal of an attacker is to compromise systems by gaining access to the network via any weak spot. There are several vulnerabilities in VPN-enabled systems, including Information Leaks, Caching and Duplication, and Denial of Service, which increase the danger of hacking a network. (Intruders' Methods, Dangers, Discoveries, and Countermeasures for Remote Access, 2010) Eavesdropping, data modification, identity spoofing (IP address spoofing), password-based assaults, man-in-the-middle, compromised-key, sniffer, and application-based attack are some more prevalent network threats.Layer Attacks are prevalent kind of network attacks. So that you may have a better grasp of typical assaults;

• Data Exposure: A problem was discovered in 2010 that was created by combining IPv6 with PPtP-based VPNs, which means that when VPN software is installed on a device, the network traffic becomes publicly exposed. (Remote Access—Attack Vectors, Threats, Findings & Remedies, 2010).

• Duplication and caching: Virtual private network (VPN) client programs may by default save your access details to make future network access easier. However, this feature puts your authentication credentials at risk and makes your sensitive data very susceptible to attacks (Remote Access—Attack Vectors, Threats, Findings & Remedies, 2010).

One of the most common types of assaults that a virtual private network (VPN) or web

- Server or any

The web server can go down due to an overwhelming number of users if proper security measures are not put in place to manage the Due to the high volume of simultaneous DDoS attempts, overload will cause the VPN to go down. If the VPN's edge network is well-protected, the VPN itself will be safe from this kind of assault. To do this, we may implement a firewall at the network level and an application layer firewall in our system. (P. Yogesh and S. Saraswathi)

• Socioeconomic Engineering The Mechanism: A social engineering assault is a one-on-one

the perpetrator convinces the victim to do something that will give him access to sensitive information, which he will then utilize in a subsequent assault. In 2010, Gregory made this claim (p. 256). Attackers often try to get in touch with the targeted individual or workers by saying they need assistance, while simultaneously contacting the IT department to request a password or that connects to the desktop remotely over the VPN communicating with the IT department to advise them of his trip plans, the nature of the situation, and the need for assistance (Gregory, 2010, p. 50) The social attacker may take advantage of this vulnerability, which is rooted in the human tendency to assist others and "be the hero," to get access to sensitive data and communicate with the targeted employee via email. The source cited is Gregory (2010) on page 101. One method of gathering sensitive information for illegal purposes is social engineering, which is tricking an individual into divulging their personal details. Credit card and bank details are the most common victims, followed by SSNs and passwords. While posing as a reliable, trustworthy source, the social engineer may communicate via email, voicemail, or even in-person visits.
(Section 1 of Social Engineering). This tells us that the hacker is after money or any information he can get

International Journal of Mechanical Engineering Research and Technology

ISSN 2454 – 535X www.ijmert.com
Vol. 16 Issue. 2, May 2024

his hands on, and that he may seek it out in a variety of ways, like sending an email, breaking into your password, or even physically showing up at your workplace. This is why it's important to lock the specific worker.If we don't fix the security holes in mobile devices, the number of assaults on these devices will only grow. To have a better grasp on the topic, we'll break down our study into two main areas. first, malware that targets iOS, and second, malware that targets Android, as these are the two most popular operating systems; has malware, there isn't a major problem with the system.because it goes against corporate policy to mess with their technology and make it open source like Android. Similar to the real game Temple Run, the malicious applications for iOS are designed to seem like Temple Climb, Temple Rush, or Cave Run. Additionally, jailbreaking is accompanied by iOS malware. rickrolled, iDevices. Malware that targets the SMS system and spammed contacts has affected both iOS and Android. (Champion and Xuan 8, 2018). Because Android is open source and anybody may create it, it has been infected with malware under the name of Droid Dream. In only four days, this virus infected 58 apps on the Android market and had 260,000 downloads. This virus mostly uses the Android debug bridge to root the phone and deliver premium SMS messages at night. As stated in Champion and Xuan's work, page 9. According to Champion and Xuan (2010, 11), Android is infested with a plethora of malware, such as the phony Angry Birds Space, bot, trojan, and Android SMS Worm, which has been propagated to all contacts using social engineering.

The Countermeasure (Chapter 6)

In order to improve the software and application security measures in the system and network, it is necessary to apply some key points. With the right risk management strategy in place, we can safeguard our company operations and keep disruptions to a minimum. To do this, we must verify many security measures, such as authentication. Remote Access: Attack Vectors, Threats, Findings, and Remedies (2010) discusses authorization and auditing. A few examples of defenses include firewalls, access controls, intrusion detection systems, and protected network cables. malware protection, Individual correspondence, Eliminate unused ports and services, Back up your data, encrypt it, install security updates, authenticate users, educate yourself, and use Unified Threats Management (UTM).

In order to improve the software and application security measures in the system and network, it is necessary to apply some key points. We need to verify certain security measures, such as those pertaining to authentication, authorization, and auditing, in order to minimize or eliminate business interruptions. This can be achieved by implementing an appropriate risk management plan (Remote Access—Attack Vectors, Threats, Findings & Remedies, 2010). If you want to improve and maintain a high degree of security measurement, you need implement access controls. These controls require sophisticated forms of TCP/IP configuration and sessions. Gregory (2010) states on page

Devices that function as firewalls were first introduced in the 1980s and were deployed on the A network's perimeter is its primary defense against unauthorized data transfers. For packets to either get through or be prevented by firewalls, they must adhere to a predetermined set of rules. Firewalls have come a long way, and the three main types are packet filters. initially implemented barriers for genreation on pass-or-their knowledge of TCP connections, stateful packet filters, and drop locations where they verify IP addresses and port numbers Firewalls of this generation are the latest iterationThis new generation of firewalls takes a step further by inspecting packets for harmful patterns or content, solving issues with the previous generation's use of smarter techniques—application layer filters. Gregory (2010) states on page 377 that The purpose of intrusion detection systems (IDS) is to monitor network traffic for malicious

International Journal of Mechanical Engineering Research and Technology

ISSN 2454 – 535X www.ijmert.com
Vol. 16 Issue. 2, May 2024

activity and notify administrators when they find it. One kind of intrusion detection system (IDS) uses a stand-alone appliance or a blade module in a network device like a router or switch. When placed on the server, host-based intrusion detection systems keep an eye out for malicious activity, such as tampering, in the form of incoming network data. Referenced in Gregory (2010), on page 377. Intrusion Prevention Systems (IPS): An IPS is a software or hardware component that acts as a watchdog, notifies the administrator of suspicious activity, and ultimately blocks the malicious traffic.IPS may be either network-based or agent-based.

Intrusion Prevention Systems (IPS) were able to detach untrusted devices from the network or block individual messages. Host-based intrusion prevention systems are software applications that may be placed on a server and are designed to detect and stop malicious events. (“Gregory, 2010, p. 378”) Avoid damage to network cables: In order to prevent unauthorized access to the network, all exposed cabling must be removed and covered. (“Gregory, 2010, p. 378”)Software that detects and blocks viruses and other malicious software will be placed on the server to ensure that the server remains safe from harm. (“Gregory, 2010, p. 378”) To safeguard systems in home or small business networks, many home-based broadband routers depend on private addressing, which is used primarily to secure publicly-routable IP addresses. According to Gregory (2010), on page 378, one of the most effective ways to decrease the likelihood of successful assaults is to close any superfluous ports or services on the system and devices.(“Gregory, 2010, p. 378”)

Servers and other network devices should have all available security patches updated as soon as possible when they become available. These patches fix bugs in the code that might leave systems vulnerable to assaults. (“Gregory, 2010, p. 378”) Security applications and devices like as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), anti-virus software, anti-spam software, and online content filters are all part of what is known as unified threat management (UTM). On page 379 of Gregory's 2010 book,
There are two layers of authentication: the first is certificate authentication, which is carried out by Alternatively, you may use a database or central directory authorization system, such as Microsoft Active Directory, to exchange certificates and/or pre-shared keys for your VPN, secret word, or password.

In highly secure contexts, two-factor authentication is necessary; this method combines the user's knowledge with their possession of an authentication certificate or token, and it effectively prevents many VPN attacks. You may lower the amount of danger by using several tokens to produce one-time passwords. (Intruders' Methods, Dangers, Discoveries, and Countermeasures for Remote Access, 2010)
When a person or system passes the authentication procedure, they are authorized to access particular network resources over the VPN. Microsoft Active Directory is one example of a popular system that can achieve this. It is critical to promptly revoke an employee's authorization when they leave the organization in order to safeguard the system. (Remote Access— Attempted Attacks, Dangers, Discoveries, and Countermeasures, 2010)
Tools are available for auditing Virtual private networks (VPNs) are handy for detecting attacks both before and after they happen, thanks to the logs that record information like: User, Coordinates of the current age, Where is the system located? The success or failure of authentication and authorization, Changing the configuration, particularly for security (intrusion detection and antivirus), Having specific access, According to Remote Access—Attack Vectors, Threats, Findings & Remedies (2010), network addresses and protocols are also important. Organizations, especially government entities, value secrecy when it comes to risk planning. In order to avoid social attacks and data leaks, it is important to have a solid risk management strategy in place. When it comes toHacking attacks may compromise security and pose a greater threat to insiders.the insider

International Journal of Mechanical Engineering Research and Technology

ISSN 2454 – 535X www.ijmert.com
Vol. 16 Issue. 2, May 2024

managed to circumvent all of the security measures put in place by the IT department and firewalls, despite their detection and protection. In order to prevent an insider threat, we may safeguard our company by The first rule is that no employee may utilize a DVD, CD-RW, detachable disc, external hard drive, or any other similar device. Malware like as viruses, spam, spyware, and Trojan horses, as well as insider threats, may be better contained with this solution.Second, you may log in with a second security authorization token in addition to a password and security questions for extra protection. Password and security question compromises may be mitigated using this. There are more than just a few of ways to verify whether the information security trying to access our system, whether they are a trusted employee or not. The first thing you need is a username and password.

To make it more difficult for an attacker to guess, use a combination of uppercase and lowercase letters, numbers, and basic symbols. Make sure the password is no more than eight characters long. To further safeguard the organization from outsiders or hackers, the second token is an authorization token that changes the security code every thirty seconds.someone attempting to get unauthorized access to data stored online, keeping tabs on where users log in, and There are a number of security systems, like as fingerprint and eye-deducting systems, that will assist to restrict access to the facility from outsiders. Timely monitoring will allow the IT staff realize whether employees are logging in to the system outside of business hours.A thorough understanding of the necessary degree of security must be developed by the IT department into a policy for security. The severity of the information security breach will vary from attack to attack. Training: Every business has to make sure its workers know what cyberattacks are and how to protect themselves. Included in this education are standard operating procedures, passwords, attack targets, and techniques. When it comes to safeguarding sensitive data, nothing beats education.

Because most assaults begin within days of a serious vulnerability being found, it is critical to apply patches to software as soon as they are found. It is necessary to visit the manufacturer's website in order to download changed software known as "patches," "security updates," or "service packs" in order to address vulnerabilities. A number of websites, including www.cert.org, maintain up-to-date listings of known vulnerabilities in critical commercial software and the fixes for them. In general, programmers have had more time to discover and repair bugs in software that has been marketed for a long amount of time, thus it's not a smart idea to acquire newly launched software items. To recover after an attack, it is vital to create copies ("backups") of digital information as many attacks delete data or programs. Any data that is considered vital should be backed up and kept at a safe distance from the systems that are being monitored. This will ensure that neither site is vulnerable to typical disasters like fire, flood, or earthquake. Storage with optical discs is better than magnetic media for backups as it is not readily destroyed. When it's critical to keep operations running smoothly, a backup might be a complete copy of the computer system.The process of encrypting data involves transforming it into an unintelligible form and then deciphering it using a string of characters called a "key" (Pfleeger & Pfleeger, 2002). You can determine if someone has tried to change an encrypted message or program since any effort to do so would render it undecipherable (or duplicated if a time is provided in the message). A new type of encryption called "public-key cryptography" has just been invented; software for it may be downloaded for free from many websites. It is strong and almost useless. Additional uses for encryption techniques include "authentication" and the provision of digital "signatures" on documents, which serve to establish the time and identity of their creator. Despite its widespread promotion, encryption is not a panacea for all security issues. Obtaining keys or disabling encryption mechanisms without your awareness is possible if an attacker acquires system-administrator capabilities.

International Journal of Mechanical Engineering Research and Technology

ISSN 2454 – 535X www.ijmert.com
Vol. 16 Issue. 2, May 2024

According to The Honeynet Project (2002) and Spitzner (2003), honeypots and honeynets (networks of honeypots) provide more detailed information on cyber-attack logs. Except for the system administrator, everyone accessing these computers is automatically suspect since they have no valid function other than to accept attackers. Does a honeypot really need to welcome attackers? Attackers may use automated methods to discover them once they are on the Internet. But if hackers use them as a stepping stone to other sites, they might do serious damage. This is why there has to be a variety of "reverse firewalls" to contain the assault. Unfortunately, a honeypot won't be able to prevent attacks indefinitely due to the fact that an attacker may deduce its presence from the limitations of the reverse firewall.

The Laws and Policies (Chapter 7)

In this chapter, it will cover the laws and the policies we have for cybersecurity. the most recent The president's executive order on cybersecurity emphasizes the gravity of the cyber threat to vital infrastructure, its ongoing growth, and the seriousness of the harm it poses to national security.

In his executive order on cybersecurity information sharing, President Obama stated that the goal of the policy is to strengthen the defenses of the private sector and make them more resilient to cyberattacks (OBAMA, 2013 Sec. 4 a). According to the National Institute of requirements and Technology (NIST) requirements for safeguarding information systems and the assets on them, every organization should strive to establish a solid risk management strategy in order to protect the valuable assets they wish to protect. In order to safeguard these assets, it is important to establish access restrictions (CRITICAL INSTRUMENT PROTECTION, 2011, pp. 11, 12). Make sure these controls are adequately tailored to these assets. Although the laws forbid all of the assaults we've described, they don't really stop them. restrictions prohibiting eavesdropping on communications and damage to computers are prevalent in many countries, including the United States. These restrictions include the majority of the assaults that we have discussed. However, most assailants do not care about being apprehended since it is difficult to trace them and the rules are not easily enforced. However, within a specific legal system, laws may be useful in preventing recurrent offenses. domain, similar to spies peddling top-secret information.The National Initiative for Cyber Security Education (NICE) classified cyber defense into seven parts: securely provisioning, operating and maintaining, protecting and defending, investigating, operating and collecting, analyzing, and supporting. We will go over each one in turn to help you comprehend and describe it better.

It is important for businesses that deal with sensitive personal information to be well-organized, particularly when it comes to information security management. It is also crucial to ensure that individuals responsible for these responsibilities understand their roles, as outlined by NICE. there are seven points in this category; To begin with, there is information assurance compliance, which means that at this stage they help the company assess, oversee, and verify that the new IT systems are up to snuff. Requirements for Additional Systems At this stage of the planning process, NICE recommends that all businesses consult with their clients to identify and evaluate their needs, and then translate those needs into practical, technically sound solutions. Additional Software

When it comes to engineering, NICE is on the side of those who design, create, and code new apps, software, or programs, as long as they meet the necessary qualifications in terms of education and technical expertise. Evaluation and Fourth Test To ensure that systems are in accordance with requirements and that they have used the techniques, all software engineers are required by NICE to conduct tests. In the fifth enterprise architecture, the capabilities of the systems development lifecycle are improved and new system ideas are created. System

International Journal of Mechanical Engineering Research and Technology

ISSN 2454 – 535X www.ijmert.com
Vol. 16 Issue. 2, May 2024

Development Phase Six Working on the development lifecycle of systems. The Seventh Technological Framework Procedures for evaluating and integrating perfume technology demonstration. In 2011, the National Initiative for Cybersecurity Education In the operational and maintenance category, developers are tasked by NICE with ensuring the system's performance and security through support, administration, and maintenance. This includes database, network, customer service, systems security analysis, and information security management skills. National Initiative for Cybersecurity Education (2011).

PROTECT AND DEFEND:

Defense in depth, including incident response, infrastructure support, vulnerability assessment and management, security program management, and computer network defense, is what NICE requires of the business in this area to protect the company's assets. In 2011, the National Initiative for Cybersecurity Education
The affected organization must conduct an investigation into the circumstances surrounding the incident and the means by which the perpetrator gained access to sensitive information. This investigation must adhere to the guidelines established by the field of digital forensics. National Initiative for Cybersecurity Education (2011). Collecting Operations, Cyber Operations, and Cyber Operations Planning are all parts of the OPERATE AND COLLECT category, which will protect them from potential intelligence development threats.

Examine: Those in charge of this domain will examine and assess cyber security data to determine its intelligence value; this includes Cyber Threat Analysis, Exploitation Analysis, All Source Intelligence, and Targets. In 2011, the National Initiative for Cybersecurity Education Assistance: Under this heading, NICE is obligated to provide assistance so that other organizations may make good use of their cybersecurity efforts. This includes providing legal counsel, advocating for better policies, and educating and training individuals. In 2011, the National Initiative for Cybersecurity Education

Reference

The authors of the article are Ahamad, M., Alperovitch, D., Conti, G., Davis, J., DeMillo, R., Feamster, N., and others (2012). Georgia Tech Emerging Cyber Threats Report 2012. The Information Security Center and the Research Institute of Georgia Tech are located in Atlanta, Georgia. Popular Forms of Attacks on Networks. [date not provided]. Source: Microsoft, retrieved March 4, 2013: http://technet.microsoft.com/en-us/library/cc959354.aspx.

“Dr. Gary Small” (n.d.). The Internet is reshaping our brains, according to studies. Retrieved January 19, 2014, from Today.UCLA.edu/portal/ut/PRN-081015_gary-small-ibrain.aspx, the University of California Los Angeles. (December 20, 2013) Hazle, M. Target suffers breach of credit card security. Retrieved

The following was released on January 14, 2014, from USC:

J. Robertson and M. Milian (2013, April 23). Cyberattacks Originating from China Climb at an Astronomical Rate. Source: http://www.bloomberg.com/news/2013-04-23/china-based-cyber-attacks-rise-at-meteoric-pace.html published by BLOOMBERG L.P. and retrieved on January 14, 2014.

(April 23, 2013) Milian and Robertson. Cyberattacks Originating from China Climb at an Astronomical Rate.

Taken down on January 21, 2014, by Bloomberg L.P.:

Chinese cyberattacks are increasing at a dizzying rate, according to a Bloomberg article published on April 23, 2013.

International Journal of Mechanical Engineering Research and Technology

ISSN 2454 – 535X www.ijmert.com
Vol. 16 Issue. 2, May 2024

The NICE stands for the National Initiative for Cybersecurity Education. on August 12, 2012.

Source: http://csrc.nist.gov/nice/framework/national_cybersecurity_workforce_framework_v1_1_, retrieved on January 21, 2014.

print-friendly August 2012 filePOTUS, B. (February 12, 2013). Executive Order—Strengthening Cybersecurity for Critical Infrastructure. The White House provided this information in an executive order aimed at enhancing the cybersecurity of vital infrastructure; it was retrieved on March 13, 2014. Prioritizing Quality in Research (1997). Data retrieved on February 28, 2014, from the following URL: http://www.okstate.edu/ag/agedcm4h/academic/aged5980a/5980/newpage21.htm published by Oklahoma State University: Remote Access—Attack Vectors, Threats, Findings & Remedies. in the year 2010. This information was retrieved on March 4, 2013, from the following source: http://www.ncp-e.com/fileadmin/pdf/techpapers/NCP-Attack-Vectors-WP.pdf. Protected by NCP.

The United Nations Telecom Agency estimates that there are over 6 billion mobile phone users worldwide (2012, 10 11). The information was retrieved on March 13, 2014, from TheHuffingtonPost.com, Inc.: http://www.huffingtonpost.com/2012/10/11/cell-phones-world-subscribers-six-billion_n_1957173.html.