INDIAN MARITIME UNIVERSITY

BASIC UNDERSTANDINGCYBER SECURITY-UGLEVEL

Chapter 1 Cyber Security

Introduction

Before high utilization of computers in the world, people suffered a lot for processing everything such as difficulty in storing and handling the huge amount of information in offices, hassle in handling money transactions in banks, delay in leading business, etc. But now-a-days, in the digital era, everything is made available to the desks of the people to do all the tasks from their places. And it has been made so easy and sophisticated with the advancements in mobile and internet technology. The word Cyber has emerged after this revolution in information technology. Cyberspace refers to the space where all the electronic devices like computers, laptops, tablets, mobile phones, etc are connected over internet. It is really a great boon to the world, however, on the other hand, the people using this technology in illegal way are increasing by leaps and pounds across the world.

The illegal way of doing all these activities using the computers, electronics devices and internet are grouped as cyber crimes. Cyber attacks are now becoming progressively destructive. In order to protect the people from the cyber attacks, cyber security is inevitable in all our daily IT related activities.

Cyber Crimes

Cybercrime is defined as "The illegal usage of any communication device to commit or facilitate in committing any illegal act". Targetting or using a computer or a group of computers under one network for the purpose of harm. A cybercriminal is a person who uses his skills in technology to do malicious acts and illegal activities known as cybercrimes. Cybercriminals are widely available in what is called the "Dark Web" where they mostly provide their illegal services or products. Cybercriminals take advantage of security holes and vulnerabilities found in systems and exploit them in order to take a foothold inside the targeted environment. Cybercrimes increases because of vulnerable devices(lack of efficient security measures), personal motivation and financial motivation. Cybercrimes can be classified into 4 categories namely Individual Cyber Crimes, Organisation Cyber Crimes, Property Cybercrimes and Society Cybercrimes.

Individual cyber crimes: targeting individuals by a person. eg:phishing, spoofing, spam, cyberstalking, and more.

Organisation Cyber Crimes: This type of crime is done by teams of criminals including malware attacks and denial of service attacks.

Property Cybercrimes: This type targets property like credit cards or even intellectual property rights.

Society Cybercrimes: This is the most dangerous form of cybercrime as it includes cyber-terrorism. A cyber crime against the government is also regarded as Cyber Terrorism. This cyber crime involves the hacking of websites, military websites, or the distribution of government propaganda.

Common forms of cybercrime include phishing, misusing personal information (identity theft),hacking, spreading hate and inciting terrorism, distributing child pornography and grooming.

Some real cyber crime incidents are discussed below for better understanding the significance of cyber security.

REvil and Kaseya Ransomware:

REvil is a Russian or Russian-speaking hacking group and it is known as a ransomware-as-a-service operation. The Kaseya incident took place in July - 2021. The incident happened when one of the Kaseya's company's products was deploying the famous SODINOKIBI REvil ransomware to endpoints of Kaseya's customer network that attack surface was over 1000 Kaseya's customers worldwide.

A few hours later REvil took credit for the attack by posting on their Happy Blog website on the dark web and demanded a $70 million ransom to release a public decryptor that they claim can decrypt all the damaged devices. The attack was so impactful that the United States government offered $10 million bounties to anyone that can give any information for arresting REvil members. Yaroslav Vasinskyi, a 22 years Ukrainian, was charged with conducting the attack and unleashing the ransomware against Kaseya and other companies.

Stuxnet:

The Stuxnet incident is a famous incident that happened in 2010. Stuxnet is the name of a computer worm (type of malware) that targets SCADA (supervisory control and data acquisition) systems.

Stuxnet malware left devastating damage to Iran’s nuclear power program. It was spreading through USB drives and affected mainly Microsoft Windows operating systems. The malware functionality was to search for machines that are working as PLCs (programmable logic controllers) and if it was found the malware updates its code over the internet through the attackers.

RockYou Data Breach:

RockYou is a company that works in the game field and was founded in 2005 by Lance Tokuda and Jia Shen. The company was working well until December 2009 when what is called “the biggest data breach of all time” happened. The data breach exposed and leaked more than 32 million user account information from RockYou database.

The company was storing passwords in an unencrypted plain text format which made it easier for the hacker to have access to all passwords stored. The hacker used a very old and popular SQL vulnerability to leak all data from the database. After this major breach, the total set of passwords that were leaked became a very helpful resource in penetration testing as hackers use this wordlist of passwords to test the security and password strength of accounts and products.

Cyber Thieves Dupe Elderly Man Case:

Noida: The Noida Police has arrested two people, allegedly involved in duping a senior citizen of ₹ 2.67 crore on the pretext of renewing his life insurance policy, almost two-and-a-half-year after the case was lodged.

Police officer said the complainant worked in an eminent private company and had retired in 2005. In 2020, the complainant got a phone call from an unknown person who informed him that his insurance policy has lapsed and he would have to pay some money if he wanted the policy renewed.Eventually, the complainant ended up paying ₹ 2.67 crore in multiple accounts in lieu of policy renewal assurance.

The complainant's daughter had filed a complaint on behalf of the senior citizen after which an FIR was lodged at the Sector 20 police station in Noida under Indian Penal Code sections 420 (fraud), 406 (criminal breach of trust) and 34 (act done by several persons) as well as the IT Act and investigation launched.

During the probe, it was found that multiple SIM cards were used in the crime and most of them were procured using forged identity cards. It took the police a lot of time to trail the miscreants but eventually they were traced and two of them have been arrested. But the duped money is yet to be recovered.

Romance Scams:

The U.S. government found this cyber threat in February 2020. Cybercriminals used this threat through dating sites, chat rooms, and apps. They attack people who are seeking a new partner and duping them into giving away personal data.

Dridex Malware:

It is a type of financial Trojan malware identifies by the U.S. in December 2019 that affects the public, government, infrastructure, and business worldwide. It infects computers through phishing emails or existing malware to steal sensitive information such as passwords, banking details, and personal data for fraudulent transactions. The National Cyber Security Centre of the United Kingdom encourages people to make sure their devices are patched, anti-virus is turned on and up to date, and files are backed up to protect sensitive data against this attack.

Emotet Malware:

Emotet is a type of cyber-attack that steals sensitive data and also installs other malware on our device. The Australian Cyber Security Centre warned national organizations about this global cyber threat in 2019.

Cyber Security

Cyber Security is a set of principles and practices designed to protect the networks, devices, programs and data from attack, theft, tamper and unauthorized access. Alternatively, it is the exercise of protecting computing resources and data over internet from malicious attacks. It is also known as information technology security or electronic information security. Based on the contexts, from business to mobile computing, where the term cyber security applies it can be classified into the following categories:

Network Security:

It involves implementing the hardware and software to secure a computer network from unauthorized access, intruders, attacks, disruption, and misuse. This security helps an organization to protect its assets against external and internal threats. eg: Firewalls, antivirus scanning devices, and content filtering.

Application Security:

It involves protecting the software and devices from unwanted threats. This protection can be done by constantly updating the apps to ensure they are secure from attacks. Different types of application security features include authentication, authorization, encryption, logging, and application security testing.

Information or Data Security:

It involves implementing a strong data storage mechanism to maintain the integrity and privacy of data, both in storage and in transit. eg. using encryption to prevent hackers from using your data.

Identity management:

It deals with the procedure for determining the level of access that each individual has within an organization. It is the practice of verifying a user's credentials, determining their access based on those credentials and how to manage users within a given system.

Operational Security:

It involves processing and making decisions on handling and securing data assets.

Mobile Security:

It involves securing the organizational and personal data stored on mobile devices such as cell phones, computers, tablets, and other similar devices against various malicious threats. These threats are unauthorized access, device loss or theft, malware, etc.

Cloud Security:

It involves in protecting the information stored in the digital environment or cloud architectures for the organization. It uses various cloud service providers such as Amazon Web Services(AWS), Azure, Google, etc., to ensure security against multiple threats.

Disaster Recovery and Business Continuity Planning:

It deals with the processes, monitors, alerts, and plans to how an organization responds when any malicious activity is causing the loss of operations or data.

End-user education:

It addresses the most unpredictable cyber security factor. Anyone can accidentally introduce a virus to a secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.

Essentials of Cyber Security

Today, in digital era, where all aspects of our lives depend on the network, computer and other electronic devices, and software applications. All critical infrastructure such as the banking system, healthcare, financial institutions, governments, and manufacturing industries use devices connected to the Internet as a core part of their operations. Some of their information, such as intellectual property, financial data, and personal data, can be sensitive for unauthorized access. This information gives intruders and threat actors to infiltrate them for financial gain, extortion, political or social motives, or just vandalism.

Cyber-attack is now an international concern that hacks the system, and other security attacks could endanger the global economy. Therefore, it is essential to have an excellent cybersecurity strategy to protect sensitive information from high-profile security breaches. Furthermore, as the volume of cyber-attacks grows, companies and organizations, especially those that deal with information related to national security, health, or financial records, need to use strong cybersecurity measures and processes to protect their sensitive business and personal information.

Cyber Security Goals

Cyber Security's main objective is to ensure data protection. The security community provides a triangle of three related principles to protect the data from cyber-attacks. This principle is called the CIA triad. The CIA model is designed to guide policies for an organization's information security infrastructure.

CIA model is divided into 3 parts namely Confidentiality, Integrity, and Availability. It is actually a security model that helps people to think about various parts of IT security.

Confidentiality: It is equivalent to privacy that avoids unauthorized access of information. It involves ensuring the data is accessible by those who are allowed to use it and blocking access to others. Data encryption is an excellent example of ensuring confidentiality.

Integrity: This principle ensures that the data is authentic, accurate, and safeguarded from unauthorized modification by threat actors or accidental user

modification. If any modifications occur, certain measures should be taken to protect the sensitive data from corruption or loss and speedy recover from such an event.

Availability: This principle makes the information to be available and useful for its authorized people always. It ensures that these accesses are not hindered by system malfunction or cyber-attacks.

Benefits of Cyber Security

- Cyberattacks and data breach protection for businesses.
- Data and network security are both protected.
- Unauthorized user access is avoided.
- After a breach, there is a faster recovery time.
- End-user and endpoint device protection.
- Regulatory adherence.
- Continuity of operations.
- Developers, partners, consumers, stakeholders, and workers have more faith in the company's reputation and trust.

Cyber Safety Tips

Some of the cyber security tips are discussed as follows:

Conduct cyber security training and awareness:

Every organization must train their staffs on cyber security, company policies, and incident reporting for a strong cyber security policy to be successful. If the staff does unintentional or intentional malicious activities, it may fail the best technical safeguards that result in an expensive security breach. Therefore, it is useful to conduct security training and awareness for staff through seminars, classes, and online courses that reduce security violations.

Update software and operating system:

The most popular safety measure is to update the software and OS to get the benefit of the latest security patches.

Use anti-virus software:

It is also useful to use the anti-virus software that will detect and removes unwanted threats from your device. This software is always updated to get the best level of protection.

Perform periodic security reviews:

Every organization ensures periodic security inspections of all software and networks to identify security risks early in a secure environment. Some popular examples of security reviews are application and network penetration testing, source code reviews, architecture design reviews, and red team assessments. In addition, organizations should prioritize and mitigate security vulnerabilities as quickly as possible once they are found.

Use strong passwords:

It is recommended to always use long and various combinations of characters and symbols in the password. It makes the passwords are not easily guessable.

Do not open email attachments from unknown senders:

The cyber expert always advises not to open or click the email attachment getting from unverified senders or unfamiliar websites because it could be infected with malware.

Avoid using unsecured Wi-Fi networks in public places:

It should also be advised not to use insecure networks because they can leave you vulnerable to man-in-the-middle attacks.

Backup data:

Every organization must periodically take backup of their data to ensure all sensitive data is not lost or recovered after a security breach. In addition, backups can help maintain data integrity in cyber-attack such as SQL injections, phishing, and ransomware.

Types of Cyber Attacks

A cyber attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft. Cyber attacks can be classified into the following categories: Web-based attacks and System-based attacks.

Web-based attacks

These are the attacks which occur on a website or web applications. Some of the important web-based attacks are as follows: Injection attacks, DNS Spoofing, Session Hijacking, Phishing, Brute force, Denial of Service, Dictionary attacks, URL Interpretation, File Inclusion attacks and Man in the middle attacks.

Injection attacks:

It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information. Example- SQL Injection, code Injection, log Injection, XML Injection etc.

DNS Spoofing:

DNS Spoofing (DNS cache poisoning) is a type of computer security hacking. It is an attack in which altered DNS records are used to redirect online traffic to a fraudulent website that resembles its intended destination. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

Session Hijacking:

It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.

Phishing:

Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading(pretending) as a trustworthy entity in electronic communication.

Brute force:

It is a type of attack which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security, analysts to test an organization's network security.

Denial of Service:

It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server. It can be classified into the following: Volume-based attacks, Protocol attacks and Application layer attacks.

Volume-based attacks- Its goal is to saturate the bandwidth of the attacked site, and is measured in bit per second.

Protocol attacks- It consumes actual server resources, and is measured in a packet.

Application layer attacks- Its goal is to crash the web server and is measured in request per second.

Dictionary attacks:

A dictionary attack is a method of breaking into a password-protected computer, network or other IT resource by systematically entering every word in a dictionary as a password.

URL Interpretation:

It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.

File Inclusion attacks:

It is a type of attack that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.

Man in the middle attacks:

It is a type of attack that allows an attacker to intercepts the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.

System-based attacks

These are the attacks which are intended to compromise a computer or a computer network. eg: Malware. Malware means malicious software, which is the most common cyber attacking tool. It is used by the cybercriminal or hacker to disrupt or damage a legitimate user's system. Some of the important system-based attacks are as follows:

Virus:

It is a malicious piece of code that spreads from one device to another. It can clean files and spreads throughout a computer system, infecting files, stoles information, or damage device.

Spyware:

It is a software that secretly records information about user activities on their system. For example, spyware could capture credit card details that can be used by the cybercriminals for unauthorized shopping, money withdrawing, etc.

Trojans:

It is a type of malware or code that appears as legitimate software or file to fool us into downloading and running. Its primary purpose is to corrupt or steal data from our device or do other harmful activities on our network.

Ransomware:

It's a piece of software that encrypts a user's files and data on a device, rendering them unusable or erasing. Then, a monetary ransom is demanded by malicious actors for decryption.

Worms:

It is a piece of software that spreads copies of itself from device to device without human interaction. It does not require them to attach themselves to any program to steal or damage the data.

Adware:

It is an advertising software used to spread malware and displays advertisements on our device. It is an unwanted program that is installed without the user's permission. The main objective of this program is to generate revenue for its developer by showing the ads on their browser.

Botnets:

It is a collection of internet-connected malware-infected devices that allow cybercriminals to control them. It enables cybercriminals to get credentials leaks, unauthorized access, and data theft without the user's permission.

Backdoors:

It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.

Types of Cyber Attackers

In computer and computer networks, an attacker is the individual or organization who performs the malicious activities to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset. As the Internet access becomes more pervasive across the world, and each of us spends more time on the web, there is also an attacker grows as well. Attackers use every tools and techniques they would try and attack us to get unauthorized access. There are four types of attackers as follows: Cyber Criminals, Hacktivists, State-Sponsored attackers and Insider threats.

Cyber Criminals:

Cybercriminals are individual or group of people who use technology to commit cybercrime with the intention of stealing sensitive company information or personal data and generating profits. In today's, they are the most prominent and most active type of attacker. Cybercriminals use computers in three broad ways to do cybercrimes:

Select computer as their target- In this, they attack other people's computers to do cybercrime, such as spreading viruses, data theft, identity theft, etc.

Uses the computer as their weapon- In this, they use the computer to do conventional crime such as spam, fraud, illegal gambling, etc.

Uses the computer as their accessory- In this, they use the computer to steal data illegally.

Hacktivists:

Hacktivists are individuals or groups of hackers who carry out malicious activity to promote a political agenda, religious belief, or social ideology. According to Dan Lohrmann, chief security officer for Security Mentor, a national security training firm that works with United States said "Hacktivism is a digital disobedience. It's hacking for a cause".

Hacktivists are not like cybercriminals who hack computer networks to steal data for the cash. They are individuals or groups of hackers who work together and see themselves as fighting injustice.

State-sponsored Attackers:

State-sponsored attackers have particular objectives aligned with either the political, commercial or military interests of their country of origin. The government organizations have highly skilled hackers and specialize in detecting vulnerabilities and exploiting these before the holes are patched. The primary goal of these hackers is to identify and exploit the national infrastructure vulnerability, gather intelligence, and exploit systems. It is very challenging to defeat these attackers due to the vast resources at their disposal.

Insider Threats:

The insider threat is a threat to an organization's security or data that comes from within. These type of threats are usually occurred from employees or former

employees, but may also arise from third parties, including contractors, temporary workers and customers. Insider threats can be categorized as follows:

Malicious threats: These are attempts by an insider to access and potentially harm an organization's data, systems or IT infrastructure. These insider threats are often attributed to dissatisfied employees or ex-employees who believe that the organization was doing something wrong with them in some way, and they feel justified in seeking revenge. Insiders may also become threats when they are disguised by malicious outsiders, either through financial incentives or extortion.

Accidental threats: These are threats which are accidently done by insider employees. In this type of threats, an employee might accidentally delete an important file or inadvertently share confidential data with a business partner going beyond company's policy or legal requirements.

Negligents: These are the threats in which employees try to avoid the policies of an organization put in place to protect endpoints and valuable data. For example, if the organization have strict policies for external file sharing, employees might try to share work on public cloud applications so that they can work at home. There is nothing wrong with these acts, but they can open up to dangerous threats nonetheless.

Types of Hackers

Hackers can be classified into three different categories:

- Black Hat Hacker
- White Hat Hacker
- Grey Hat Hacker

Black-hat Hackers:

They are also known as an Unethical Hacker or a Security Cracker. These people hack the system illegally to steal money or to achieve their own illegal goals. They find banks or other companies with weak security and steal money or credit card information. They can also modify or destroy the data as well. Black hat hacking is illegal.

White hat Hackers:

They are also known as Ethical Hackers or a Penetration Tester. White hat hackers are the good guys of the hacker world. These people use the same technique used by the black hat hackers. They also hack the system, but they can only hack the system that they have permission to hack in order to test the security of the system. They focus on security and protecting IT system. White hat hacking is legal.

Gray hat Hackers:

They are Hybrid between Black hat Hackers and White hat hackers. They can hack any system even if they don't have permission to test the security of the system but they will never steal money or damage the system. In most cases, they tell the administrator of that system. But they are also illegal because they test the security of the system that they do not have permission to test. Grey hat hacking is sometimes acted legally and sometimes not.

Different types of Web

Web(World Wide Web) means a complex system of interconnected elements. A website is a collection of interlinked web pages with a common domain name. The website can be made by any individual, group, or company. All the websites together constitute the world wide web. Every website has several linked web pages. The

structure of a web page was made using HTML, a hypertext markup language. The domain name categorizes the types of websites: commercial websites used .com extension and non-profit organization used .org extension. There are so many types of websites available among which some are basic websites:

Personal website:

- used for sharing your personal information
- used for sharing your philosophical thoughts and showcase your work
- used to brand themselves.

Photo sharing website:

It enables you to store your photographs online and share them with your family and friends. Here one can upload as much as they want, also manage it as well as share it (private or public).

Blog:

A blog is a website where people share information, ideas, and views. Earlier, blogs were used as a journal, but now they are becoming one of the important mass communication tools where people get to know about new things. WordPress and Google blogger are famous blogging sites where you can write articles. Blogs include a travel blog, news blog, cooking blog, etc.

Informational website:

This website provides information on various topics. For example, Wikipedia is an information website where you can get information about everything related to history, geography, science and technology, cinema, famous people, etc.

E-Commerce website:

This is the place for online shopping where a person can buy or sell a product. Amazon, Flipkart, and Olx are some of the examples of an E-commerce website.

Social Media website:

This is the most popular website where people can connect with each other. Social media websites enable the user to share their personal information, pictures, video ideas, and opinion in real-time. Facebook, Instagram, and Twitter are some examples of social media websites.

Educational Websites:

Education websites include websites of colleges and schools and tuitions. Nowadays, people are learning through online classes and the demands of educational websites also grow. eg. Coursera, GeeksforGeeks, NPTEL, edX, etc.

Portfolio Websites:

These websites are used to showcase your best work to a professional. A portfolio website is a majorly creative one. For example, I am a writer and I want a job in digital content writing. Then I can make a portfolio website where I can showcase my different type of writing style on the website.

Non-Profit website:

Like profit organizations, non-profit organizations also need the attention of public. This is the reason behind the emerging of these websites. Every NGO has its own website. They use them to inform their audience, raising funds, and also informing about themselves what they are doing. eg. gatesfoundation.org is a non-profit website.

Magazine and News Websites:

Many people got confused with a blog website and news websites. Basically, a news website focused on journalism rather than personal interests. News and magazine websites monetize through advertisement and subscription models. For

example, The Times of India have their own website called timesofindia.indiatimes.com where you can read news online.

Chapter 2 Cyber security key aspects

Cyber Security Vulnerability

A vulnerability in cyber security is a weakness in a host or system, such as a missed software update or system misconfiguration, that can be exploited by cybercriminals to compromise an IT resource and advance the attack path. Identifying cyber vulnerabilities is one of the most important steps that organizations can take to improve and strengthen their overall cyber security posture.

Most of us use the terms vulnerability, threat and risk interchangeably. However, in the cyber security world, these terms have distinct and specific meanings. A threat is a malicious act that can exploit a security vulnerability**.** A risk is what happens when a cyber threat exploits a vulnerability. It represents the damage that could be caused to the organization in the event of a cyberattack. A vulnerability is a weakness that can be exploited by a malicious actor. For example, unpatched software or overly permissive accounts can provide a gateway for cybercriminals to access the network and gain a foothold within the IT environment.

Few examples of cyber security vulnerabilities: Missing data encryption, Lack of security cameras, Unlocked doors at businesses, Unrestricted upload of dangerous files, Code downloads without integrity checks, Using broken algorithms, URL Redirection to untrustworthy websites, Weak and unchanged passwords and Website without Secure Socket Layer(SSL).

Causes of Cyber Security Vulnerabilities

The causes of cyber security vulnerabilities are as follows:

Complexity: The likelihood of errors, defects, or unauthorized access increases with complex systems.

Familiarity: Attackers may already be acquainted with common code, operating systems, hardware, and software that result in well-known vulnerabilities.

Connectivity: Vulnerabilities are more likely to exist in connected devices. It is better to avoid connecting to multiple devices unnecessarily.

Poor Password Management: This can cause several data breaches because of weak or repeated passwords. It is important to change passwords using strong password generators regularly.

Internet: Spyware and adware that can be loaded on computers automatically are abundant on the internet.

Operating System Flaws: Operating systems can also be flawed. Operating systems that aren't safe by default might provide users unrestricted access and serve as a heaven for malware and viruses.

Software Bugs: Sometimes, programmers may unintentionally introduce a vulnerability that can exploit.

Unchecked User Input: If software or a website presumes that all user input is secure, SQL injection may be executed without the user's knowledge.

People: For most organizations, social engineering poses the biggest concern. Therefore, one of the main sources of vulnerability can be people.

Types of Cyber Vulnerabilities

When reviewing one company's cybersecurity posture and approach, it's important to realize that cybersecurity vulnerabilities are within the control of the organization — not the cybercriminal. There are seven most common types of cyber vulnerabilities and let us study how organizations can neutralize them.

Misconfigurations:

Misconfigurations are the single largest threat to both cloud and app security. Because many application security tools require manual configuration, this process can be rife with errors and take considerable time to manage and update. In recent years, numerous publicly reported breaches started with misconfigured S3 buckets(public cloud storage resource) that were used as the entry point. The absence of perimeter security within the cloud further compounds the risk associated with misconfigurations. Hence, it is important for organizations to adopt security tooling and technologies and automate the configuration process and reduce the risk of human error within the IT environment.

Unsecured APIs:

Another common security vulnerability is unsecured application programming interfaces (APIs). APIs provide a digital interface that enables applications or components of applications to communicate with each other over the internet or via a private network. APIs are one of the few organizational assets with a public IP address. If not properly and adequately secured, they can become an easy target for attackers to breach. As with misconfigurations, securing APIs is a process prone to human error. IT teams may simply be unaware of the unique security risk. Conducting a security awareness training to educate teams on security best practices specific to the cloud — such as how to store secrets, how to rotate keys and how to practice good IT hygiene during software development — is critical in the cloud, just as in a traditional environment.

Outdated or Unpatched Software:

Software vendors periodically release application updates to either add new features and functionalities or patch known cybersecurity vulnerabilities. Unpatched or outdated software often make for an easy target for advanced cybercriminals. While software updates may contain valuable and important security measures, it is the responsibility of the organization to update their network and all endpoints.

Unfortunately, because updates from different software applications can be released daily and IT teams are typically overburdened, it can be easy to fall behind on updates and patching, or miss a new release entirely. Failing to update even one machine can have potentially disastrous consequences for the organization, providing an attack path for ransomware, malware and a host of other security threats. To help address this issue, organizations should develop and implement a process for prioritizing software updates and patching. To the extent possible, the team should also automate this activity so as to ensure systems and endpoints are as up to date and secure as possible.

Zero-day Vulnerabilities:

A zero-day vulnerability refers to a security flaw that has been discovered by a threat actor but is unknown to the enterprise and software vendor. The term “zero-day” is used because the software vendor was unaware of their software vulnerability, and they’ve had “0” days to work on a security patch or an update to fix the issue; meanwhile it is a known vulnerability to the attacker. Zero-day attacks are extremely dangerous for companies because they can be very difficult to detect.

To effectively detect and mitigate zero-day attacks, a coordinated defense is needed — one that includes both prevention technology and a thorough response plan in the event of a cyberattack. Organizations can prepare for these stealthy and damaging events by deploying a complete endpoint security solution that combines technologies including next-gen antivirus (NGAV), endpoint detection and response (EDR) and threat intelligence.

Weak or Stolen User Credentials:

Many users fail to create unique and strong passwords for each of their accounts. Reusing or recycling passwords and user IDs creates another potential avenue of exploitation for cybercriminals. Weak user credentials are most often exploited in brute force attacks when a threat actor tries to gain unauthorized access to sensitive data and systems by systematically trying as many combinations of usernames and guessed passwords as possible. If successful, the actor can enter the system and masquerade as the legitimate user; the adversary can use this time to move laterally, install back doors, gain knowledge about the system to use in future cyberattacks, and, of course, steal data.

To address this particular cybersecurity vulnerability, organizations should set and enforce clear policies that require the use of strong, unique passwords and prompt users to change them regularly. Organizations should also consider implementing a multifactor authentication (MFA) policy, which requires more than one form of identification, such as both a password and a fingerprint or a password and a one-time security token, to authenticate the user.

Access Control or Unauthorized Access:

Companies often grant employees more access and permissions than needed to perform their job functions. This increases identity-based threats and expands access to adversaries in the event of a data breach. To address this issue, organizations should implement the Principle of Least Privilege (POLP), a computer security concept and practice that gives users limited access rights based on the tasks necessary to their job. POLP ensures only authorized users whose identity has been verified have the necessary permissions to execute jobs within certain systems, applications, data and other assets.

POLP is widely considered to be one of the most effective practices for strengthening the organization's cybersecurity posture, in that it allows organizations to control and monitor network and data access.

Misunderstanding the Shared Responsibility Model (Runtime Threats):

Cloud networks adhere to what is known as the "shared responsibility model." This means that much of the underlying infrastructure is secured by the cloud service provider. However, the organization is responsible for everything else, including the operating system, applications and data. Unfortunately, this point can be misunderstood, leading to the assumption that cloud workloads are fully protected by the cloud provider. This results in users unknowingly running workloads in a public cloud that are not fully protected, meaning adversaries can target the operating system and the applications to obtain access.

Organizations that are using the cloud or shifting to a cloud or hybrid work environment must update their cybersecurity strategy and tooling to ensure they are protecting all areas of risk across all environments. Traditional security measures do not provide security in a cloud environment and must be supplemented to provide enhanced protection from cloud-based vulnerabilities and threats.

Cyber Security Safeguards

Cyber security safeguards are all kind of control measures that support the fulfillment of requirements or the achievement of objectives related to cyber security. Safeguards can be functionally distinguished in administrative, technical safeguards and physical safeguards, shown in Figure 2.1.

Administrative safeguards include all activities that do not necessarily have to be carried out by technical means. Examples are guidelines, trainings, manual controls

and planning measures. The effectiveness of these safeguards depends on the awareness and the acceptance of the employees.

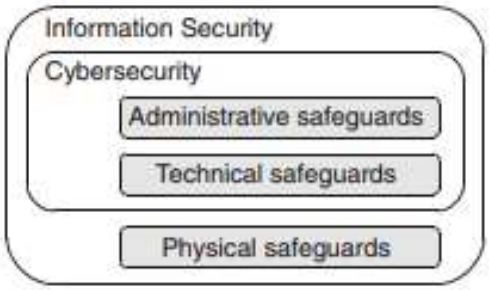

Figure 2.1 Functional classification of cybersecurity safeguards

Technical safeguards are supported or enabled by technical means, like antivirus software and access control systems. In many cases, the operation of technical safeguards can be automated, e.g. antivirus software can move a malicious program in quarantine or delete it without manual action.

Physical safeguards that are not part of cybersecurity in the narrower sense, but rather part of the more general field of information security. Physical safeguards are used to protect the physical perimeter and infrastructure of a company. e.g. fences, security guards, security cameras, fire-fighting equipment, uninterruptible power supplies and flood protection mechanisms.

Another way for distinguishing safeguards is the perspective of time. From this perspective, they can be preventive, detective or corrective, shown in Figure 2.2.

Figure 2.2 Classification of cybersecurity safeguards based on time

Preventive safeguards become effective before an event occurs. Generally, they are the first choice in cybersecurity because negative impacts and resulting damages can be completely avoided.

Detective safeguards become effective while an event occurs. They often trigger corrective safeguards.

Corrective safeguards become effective after an event occurs. They are used to correct the negative effects of adverse events.

From the combined perspectives of function and time, six different safeguard types as shown in Table 2.1, can be derived.

It is impossible to achieve 100% protection from cyber crimes. The focus is, however, to minimize their occurrence and the resulting losses.

Some common measures to safeguard ourselves are listed below. We can divide them into two categories:

i. Strengthening security over the Internet
ii. Strengthening security of a web site

Table 2.1 Types of cybersecurity safeguards based on function and time

Safeguards	Administrative	Technical
Preventive	Policies and Procedures Need to Know Separation of Duties Awareness and Training Background Checks Data Classification Revision Control Outsourcing	Access Control Systems Application Control Network Security Hardening Secure Software Development Encryption Data Leakage Prevention Technical Resilience
Detective	ncident Management Testing Supervising Job Rotation and Vacation Reporting	Malware Protection Intrusion Detection Systems File Integrity Monitoring Audit Trails
Corrective	Business Continuity Management Software Escrow Incident Response Insurances	Patch Management Disaster Recovery Backups Journaling File System

In order to reinforce Internet security, the following measures are used.

i. Encryption
ii. Digital signatures
iii. Secure Web servers
iv. Anti-Virus software
v. Security in Internet Explorer

Encryption: It is the process of scrambling data which is transmitted in an unreadable format. This process converts the original representation of the information(plaintext) into an alternative form known as ciphertext. The data has to be unscrambled or decrypted in order to be converted back into readable format.To achieve this, the user needs to have a key or password which reverses the process of encryption.

Digital signatures: Though encrypted files can be used to verify that the person sending you the file is known to you, sometimes using digital signatures is more efficient. Digital signature also called as e-signature. This ensures that the file or message was not altered since it was signed. Digital signatures are based on Public Key Infrastructure (PKI) and guarantees signer authenticity. The digital signature cannot be copied, tampered or altered.

Secure Web servers: Sensitive Internet transactions such as online shopping, stock trading, banking etc should only be performed via Web pages that use some kind of encryption or some appropriate security method. The way to find out if a web page is secure or not is to look for an icon of a locked padlock which is normally located on the bottom right of status bar. Also, the URL of the secure Web page begins with https:// instead of http://.

Anti-virus software: A variety of anti-virus software are available that prevent virus programs from attacking your computer. However, it is always prudent to buy the latest anti-virus software from well known software dealers such as Norton Utilities, McAfee Antivirus and so on. One must run regular updates to keep the anti-virus protection up-to-date since new viruses are constantly being written by malicious hackers.

Security in Internet Explorer and e-mails: Digital certificates(SSL certificates) are authentication for an individual or business web site, and are available from any certificate authority such as VeriSign, PrivacyX, or Equifax. A server certificate ensures that the data transfer between the user's computer and the server is tamper-proof and free from being intercepted.

Strengthening security of a website

In order to reinforce the security of a web site, we could perform the following:

i. Configure the security features of a web page
ii. Understand the role of cookies

Before sending sensitive information such as credit card numbers, addresses, phone numbers, and social security numbers over the Internet, one should check if the Web page will be encrypted during its transmission from the Web server. The following figures will show how to identify an authentic website. To view the certificate, you need to click on the menu option called "view", and then click "Security report" & "View certificate". These dialog boxes indicate that the website is verified.

Digital certificate in Internet Explorer- General tab is shown in Figure 2.3 and Digital certificate in Internet Explorer- Details tab is shown in Figure 2.4.

Figure 2.3 Digital certificate in Internet Explorer- General tab

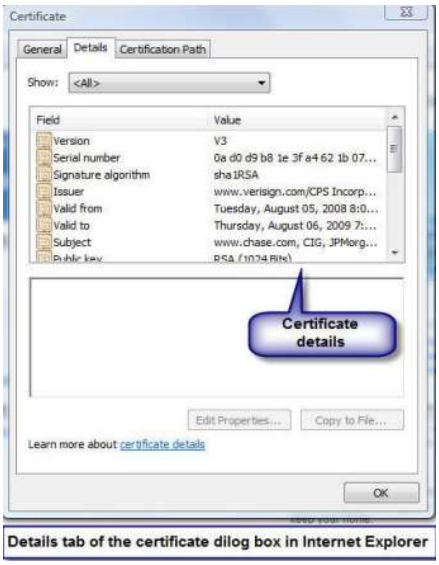

Figure 2.4 Digital certificate in Internet Explorer- Details tab

Understanding the role of cookies: A cookie is a small electronic text file stored on your hard drive. Cookies are used by the Web sites to keep a track of any information

that the browser will need on a future visit. The cookie might silently record your behavior on a Website. Only the Website that recorded a cookie on your hard drive can read it, it cannot read other cookies or other files on your computer. That's the reason, they say, cookies are harmless. However, you can delete the cookies after your session is over. Most browsers provide you with that option.

Steps to Keeping Your Computer Safe on the Internet:

- Use a Firewall
- Scan for Viruses
- Scan for Spyware
- Stay Up-To-Date
- Don't open suspicious attachments or click unusual links in messages.
- Make sure your passwords are well-chosen and protected
- Secure Your Home Network and Your Mobile Connection
- Stay away from pirated material
- Back Up data periodically

Securing Web Application, Services and Servers

Web application security is the practice of protecting websites, applications, and APIs from attacks. It is a broad discipline, but its ultimate aims are keeping web applications functioning smoothly and protecting business from cyber vandalism, data theft, unethical competition, and other negative consequences. Web applications may face a number of attack types depending on the attacker's goals, the nature of the targeted organization's work, and the application's particular security gaps.The most common types of cyber attacks are as follows:

Zero-day vulnerabilities:

These are vulnerabilities unknown to an application's makers, and which thus do not have a fix available. Attacks look to exploit these vulnerabilities quickly, and often follow up by seeking to evade protections put in place by security vendors.

Cross site scripting (XSS):

XSS is a vulnerability that allows an attacker to inject client-side scripts into a webpage viewed by other users in order to access important information directly, impersonate the user, or trick the user into revealing important information.

SQL injection (SQi):

SQi is a method by which an attacker exploits vulnerabilities in the way a database executes search queries. Attackers use SQi to gain access to unauthorized information, modify or create new user permissions, or otherwise manipulate or destroy sensitive data.

Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks:

Through a variety of vectors, attackers are able to overload a targeted server or its surrounding infrastructure with different types of attack traffic. When a server is no longer able to effectively process incoming requests, it begins to behave sluggishly and eventually deny service to incoming requests from legitimate users.

Memory corruption:

Memory corruption occurs when a location in memory is unintentionally modified, resulting in the potential for unexpected behavior in the software. Bad actors will attempt to sniff out and exploit memory corruption through exploits such as code injections or buffer overflow attacks.

Buffer overflow:

Buffers are memory storage regions that temporarily hold data while it is being transferred from one location to another.

A buffer overflow occurs when the volume of data exceeds the storage capacity of the memory buffer. Overflowing the buffer's capacity results in adjacent memory locations being overwritten with data. This behavior can be exploited to inject malicious code into memory, potentially creating a vulnerability in the targeted machine.

Cross-site request forgery (CSRF):

Cross site request forgery involves tricking a victim into making a request that utilizes their authentication or authorization. For example, this might be to change the email address on their account, to change their password, or to make a funds transfer. By leveraging the account privileges of a user, an attacker is able to send a request masquerading as the user. Once a user's account has been compromised, the attacker can exfiltrate, destroy or modify important information. Highly privileged accounts such as administrators or executives are commonly targeted.

Credential stuffing:

Attackers may use bots to quickly input large numbers of stolen username and password combinations into a web application's login portal. For example, an attacker may take a list of usernames and passwords obtained from a breach of a major department store, and use the same login credentials to try and log in to the site of a national bank. The attacker is hoping that some fraction of those department store customers also have an account at that bank, and that they reused the same usernames and passwords for both services. This practice gives the attacker access to a real user's account, they may steal the user's data or make fraudulent purchases in the user's name.

Page scrapping:

It is also known as Web scrapping. Attackers may use bots to steal content from webpages on a large scale. It extracts underlying HTML code and, with it, data stored in a database. They may use this content to gain a pricing advantage over a competitor, imitate the page owner for malicious purposes, or other reasons. Web Scrapers can extract all the data on particular sites or the specific data that a user wants. For example, you might want to scrape an Amazon page for the types of juicers available. It is very helpful for companies in analyzing consumer trends and understanding which direction the company should move in the future.

API abuse:

APIs, or Application Programming Interfaces, are software that allow two applications to communicate with each other. Like any type of software, they may have vulnerabilities that allow attackers to send malicious code into one of the applications or intercept sensitive data as it moves from one application to another. This is an increasingly common attack type as API use increases.

Shadow APIs:

Development teams work quickly to meet business objectives, frequently building and publishing APIs without informing security teams. These unknown APIs may expose sensitive company data, operating in the "shadows", as security teams tasked with protecting APIs are unaware of their existence.

Third-party code abuse:

Many modern web applications use a variety of third-party tools — for example, an ecommerce site using a third-party payment processing tool. If attackers find a vulnerability in one of these tools, they may be able to compromise the tool, and steal the data it processes, prevent it from functioning, or use it to inject malicious code elsewhere in the application.

Magecart attacks:

They skim credit card data from payment processors, are an example of this attack type. These attacks are also considered to be browser supply chain attacks.

Important web application security strategies

DDoS mitigation:

DDoS mitigation services sit between a server and the public Internet, using specialized filtration and extremely high bandwidth capacity to prevent surges of malicious traffic from overwhelming the server. These services are important because many modern DDoS attacks deliver enough malicious traffic to overwhelm even the most resilient servers.

Web Application Firewall (WAF):

It filters out traffic known or suspected to be taking advantage of web application vulnerabilities. WAFs are important because new vulnerabilities emerge too quickly and quietly for nearly all organizations to catch on their own.

Web application security products and policies strive to protect applications through measures such as web application firewalls (WAFs), multi-factor authentication (MFA) for users, validation of cookies to maintain user state and privacy status, and various methods for validating user input.

The primary target is the application layer (i.e., what is running on the HTTP protocol). HTTP stands for Hypertext Transfer Protocol. Hypertext Transfer Protocol is a set of rule which is used for transferring the files like, audio, video, graphic image, text and other multimedia files on the WWW (World Wide Web). HTTP is used to communicate over the internet, so users, information providers, and application developers should be aware of the limitations of security in HTTP.

In HTTP, clients are often privy to a large amount of personal information like: name of the user, email address, passwords, location, Encryption key, etc. We should be careful to prevent unintentional leakage of this personal information of the client via the HTTP protocol to other sources.

A WAF protects web applications from a variety of application layer attacks such as cross-site scripting (XSS), SQL injection, and cookie poisoning, among others. A WAF protects your web apps by filtering, monitoring, and blocking any malicious HTTP/S traffic traveling to the web application, and prevents any unauthorized data from leaving the app. It does this by adhering to a set of policies that help determine what traffic is malicious and what traffic is safe. Just as a proxy server acts as an intermediary to protect the identity of a client, a WAF operates in similar fashion but in the reverse—called a reverse proxy—acting as an intermediary that protects the web app server from a potentially malicious client. WAFs can come in the form of software, an appliance, or delivered as-a-service.

API gateways:

They help identify overlooked ‘shadow APIs,’ and block traffic known or suspected to target API vulnerabilities. They also help manage and monitor API traffic.

DNSSEC(Domain Name System Security Extensions):

A protocol which guarantees a web application’s DNS traffic is safely routed to the correct servers, so users are not intercepted by an on-path attacker.

Encryption certificate management:

In which a third party manages key elements of the SSL/TLS encryption process, such as generating private keys, renewing certificates, and revoking certificates due to vulnerabilities. This removes the risk of those elements going

overlooked and exposing private traffic. Secure Socket Layer(SSL) and Transport Layer Security(TLS) are encryption protocols that protect internet communications.

Bot management:

Bot management refers to blocking undesired or malicious Internet bot traffic while still allowing useful bots to access web properties. Bot management accomplishes this by detecting bot activity, discerning between desirable and undesirable bot behavior, and identifying the sources of the undesirable activity.

Client-side security:

It refers to the technologies and policies used to protect an end user from malicious activity that is occurring on dynamic web pages accessed from the end user's own device.

Attack surface management:

An attack surface is defined as the total number of all possible entry points for unauthorized access into any system. Actionable attack surface management tools should provide a single place to map your attack surface, identify potential security risks, and mitigate risks with a few clicks.

Intrusion Detection and Prevention

Intrusion Detection System (IDS):

An IDS is a security system which monitors the computer systems and network traffic. It analyses that traffic for possible hostile attacks originating from the outsider and also for system misuse or attacks originating from the insider. Like, the firewall protects an organization sensitive data from malicious attacks over the Internet, the Intrusion detection system alerts the system administrator in the case when someone tries to break in the firewall security and tries to have access on any network in the trusted side.

Types of IDS:

There are basically two types of IDS namely Network Intrusion Detection System (NIDS) and Host Intrusion Detection System (HIDS).

NIDS :

It is a Network Intrusion Detection System which monitors the inbound and outbound traffic to and from all the devices over the network.

HIDS:

It is a Host Intrusion Detection System which runs on all devices in the network with direct access to both internet and enterprise internal network. It can detect anomalous network packets that originate from inside the organization or malicious traffic that a NIDS has failed to catch. HIDS may also identify malicious traffic that arises from the host itself.

Based on working mechanism, IDS can be classified as follows:

Signature-based Intrusion Detection System:

It is a detection system which refers to the detection of an attack by looking for the specific patterns, such as byte sequences in network traffic, or known malicious instruction sequences used by malware. This IDS originates from anti-virus software which can easily detect known attacks. In this terminology, it is impossible to detect new attacks, for which no pattern is available.

Anomaly-based Intrusion Detection System:

This detection system primarily introduced to detect unknown attacks due to the rapid development of malware. It alerts administrators against the potentially malicious activity. It monitors the network traffic and compares it against an established

baseline. It determines what is considered to be normal for the network with concern to bandwidth, protocols, ports and other devices.

Intrusion Prevention System (IPS):

It is also known as Intrusion Detection and Prevention System. It's a network security program that looks for harmful activity on a network or system. Intrusion prevention systems' main functions are detecting malicious behavior, collecting information about it, reporting it, and trying to block or stop it. IPS is shown in Figure 2.5.

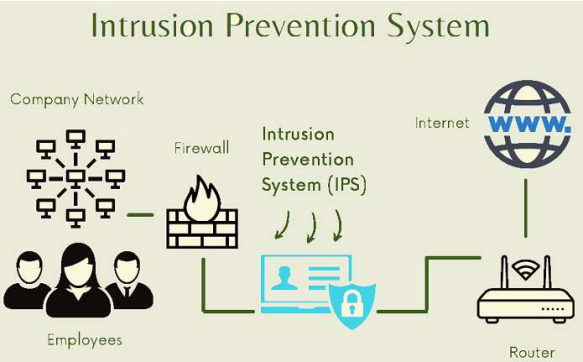

Figure 2.5 Intrusion Prevention System

IPS normally logs information about observed events, notifies security administrators about significant occurrences, and generates reports. Many IPS can also try to prevent a threat from succeeding if it has been discovered. They utilize various response strategies, including the IPS interrupting the attack, modifying the security environment, and changing the substance of the attack.

Working of IPS:

The IPS thoroughly inspects every packet that travels across the network in real-time. If the IPS detects any malicious or suspicious packets, it will take one of the following actions:

- Terminate the compromised TCP session and block the offending source IP address or user account from accessing any application, target hosts, or other network resources in an unethical manner.
- Reprogram or adjust the firewall to avoid future attacks of this nature.
- Removes or replaces any dangerous content that is found on the network after an attack. This is accomplished by repackaging payloads, removing header information, and removing any malicious attachments from file or email servers.

Advantages of IPS:

- Lowering the likelihood of security incidents
- Providing dynamic threat protection
- Defending against zero-day threats, distributed denial-of-service attacks, and brute-force attacks
- Informing admins automatically when questionable activity is discovered
- Permitting or refusing certain inbound traffic to a network
- Reducing network maintenance for IT workers.

Drawbacks of IPS:

- When a system detects unusual network activity and assumes it is malicious, it may be a false positive, resulting in a DoS attack on an innocent user.
- If an organization's bandwidth and network capacity are insufficient, an IPS tool may slow down a system

- If a network has numerous IPS, data must transit through each to reach the end-user, which may reduce network performance.
- IPS is more costly than others.

Types of Prevention Mechanism:

To defend the network from unauthorized access, an intrusion prevention system is usually set up to use various methods. These are some of them:

Signature-Based:

The signature-based technique employs predefined signatures of well-known network hazards. When an attack is launched that matches one of these signatures or patterns, the system reacts.

Anomaly-Based:

The anomaly-based strategy keeps an eye on the network for any unusual or unexpected activity. The system immediately disables access to the target host if an abnormality is identified.

Policy-Based:

Administrators must configure security policies by organizational security policy and network infrastructure in this manner. When behaviour that violates a security policy occurs, an alert is triggered and sent to the system administrators.

In signature-based detection mechanism, intrusion prevention systems use a dictionary of individually identifiable signatures detected in the code of each exploit. There are two types of signature-based detection approaches for intrusion prevention systems: exploit-facing and vulnerability-facing. Detecting harmful activity by identifying individual vulnerabilities is the goal of exploit-facing methodologies, whereas detecting malicious activity by detecting common attack patterns is the goal of vulnerability-facing methods.

Classification of IPS:

The network-based interruption anticipation framework (NIPS) analyses protocol activity to monitor the entire network for suspicious traffic.

Wireless interruption anticipation framework (WIPS) analyzes wireless networking protocols to keep an eye on suspicious traffic on a wireless network.

Network Behavior Analysis (NBA): It analyses network data to look for threats that cause odd traffic patterns, such as distributed denial of service assaults, certain types of malware, and policy violations.

Host-based interruption anticipation framework (HIPS):It's a built-in software package that monitors a single host for suspicious behavior by examining events that take place on that host.

Difference between IDS and IPS:

An IDS is designed to only provide an alert about a potential incident, which enables a security operations center (SOC) analyst to investigate the event and determine whether it requires further action. An IPS, on the other hand, takes action itself to block the attempted intrusion or otherwise remediate the incident.

The following features differentiate IPS and IDS:

- Intrusion prevention systems are deployed in-line and can actively prevent or block suspected invasions.
- An IPS can issue an alert drop malicious identifications packets, re-establish a connection, or block traffic from the attacker's IP address.

- IPS can also defragment packet streams, reduce TCP sequencing difficulties, clean out unwanted transport and network layer options, and repair CRC errors.

Cyberspace and the Law

The term Cyberspace seemed to have originated from a Science fiction movie. However, in the 21st century, it has become an integral part of our lives. The best way to define Cyberspace is the virtual and dynamic space created by the machine clones. According to the Cyberspace definition, it is a web consisting of consumer computers, electronics and communication networks by which the consumer is connected to the world. Cyberspace can be compared to a human brain where the network of computers represent the innumerable neurons and the connections between them. Therefore, it can be considered as a link between the physical and the infinite world.

Cyber Laws and Cyber Security:

In order to ensure that humans do not misuse Cyber technologies, Cyber laws are generated. The overall idea of Cyberlaw is to stop any person from violating the rights of other persons in Cyberspace. Any kind of violation of Cyber rights is considered to be a Cyberspace violation and is deemed punishable under Cyber Laws. A separate set of Cyber laws are formulated by the government to provide cyber security to Cyber users. Cyber laws are needed to monitor and prevent any immoral or illegal activities of humans like hacking, theft, money laundering, terrorism, piracy, etc.

Cyber laws encompass all the legal issues related to the communicative, distributive and transactional aspects of network-related information devices and technologies. Cyber laws are related to individuals and institutions that

- Play a crucial role in providing Cyberspace access to people
- Generates software and/or hardware to allow people with entry into Cyberspace, and
- Make use of their computer system to gain entry into Cyberspace.

To define the different arms of Cybersecurity, two main acts are considered in India. They are:

- The Indian Penal Code, 1860
- The Information Technology Act, 2000

The Information Technology Act, 2000 was enacted by the Indian Parliament in 2000. It is the primary law in India for matters related to cybercrime and e-commerce. The act was enacted to give legal sanction to electronic commerce and electronic transactions, to enable e-governance, and also to prevent cybercrime. Under this law, for any crime involving a computer or a network located in India, foreign nationals can also be charged. The law prescribes penalties for various cybercrimes and fraud through digital/electronic format.

It also gives legal recognition to digital signatures. The IT Act also amended certain provisions of the Indian Penal Code (IPC), the Banker's Book Evidence Act, 1891, the Indian Evidence Act, 1872 and the Reserve Bank of India Act, 1934 to modify these laws to make them compliant with new digital technologies. In the wake of the recent Indo-China border clash, the Government of India banned various Chinese apps under the Information Technology Act.

Cyber laws are formed to punish people who perform any illegal activities online such as online harassment, attacking another website or individual, data theft, disrupting the online workflow of any enterprise and other illegal activities. If anyone

breaks a cyber law, the action would be taken against that person on the basis of the type of cyberlaw he broke, where he lives, and where he broke the law. It is most important to punish the criminals or to bring them to behind bars, as most of the cybercrimes cross the limit of crime that cannot be considered as a common crime. These crimes may be very harmful for losing the reliability and confidentiality of personal information or a nation. Therefore, these issues must be handled according to the laws.

There are various broad categories that come under cyber laws; some are as follows:

Fraud:

Cyber laws are formed to prevent financial crimes such as identity theft, credit card theft and other that occurring online. A person may face confederate criminal charges if he commits any type of identity theft. These laws have explained strict policies to prosecute and defend against allegations of using the internet.

Copyrighting Issues:

The Internet is the source that contains different types of data, which can be accessed anytime, anywhere. But it is the authority of anyone to copy the content of any other person. The strict rules are defined in the cyber laws if anyone goes against copyright that protects the creative work of individuals and companies.

Scam/ Treachery:

There are different frauds and scams available on the Internet that can be personally harmful to any company or an individual. Cyber laws offer many ways to protect people and prevent any identity theft and financial crimes that happen online.

Chapter 3 Security protocol and implementation

Cyber Forensics

Cyber forensics is a process of extracting data as proof for a crime (that involves electronic devices) while following proper investigation rules to nab the culprit by presenting the evidence to the court. Alternatively, the science of collecting, inspecting, interpreting, reporting, and presenting computer-related electronic evidence is known as cyber forensics. Evidence can be found on the hard drive or in deleted files. It is the process of examining, acquiring, and analyzing data from a system or device so that it can be transcribed into physical documentation and presented in court.

Cyber forensics is also known as computer forensics. The main aim of cyber forensics is to maintain the thread of evidence and documentation to find out who did the crime digitally. Cyber forensics can do the following:

- It can recover deleted files, chat logs, emails, etc
- It can also get deleted SMS, Phone calls.
- It can get recorded audio of phone conversations.
- It can determine which user used which system and for how much time.
- It can identify which user ran which program.

Importance of Cyber Forensics:

- Cyber forensics helps in collecting important digital evidence to trace the criminal.
- Electronic equipment stores massive amounts of data that a normal person fails to see. For example: in a smart house, for every word we speak, actions performed by smart devices, collect huge data which is crucial in cyber forensics.
- It is also helpful for innocent people to prove their innocence via the evidence collected online.
- It is not only used to solve digital crimes but also used to solve real-world crimes like theft cases, murder, etc.
- Businesses are equally benefitted from cyber forensics in tracking system breaches and finding the attackers.

Process Involved in Cyber Forensics:

- Obtaining a digital copy of the system that is required to be inspected.
- Authenticating and verifying the reproduction.
- Recovering deleted files (using Autopsy Tool).
- Using keywords to find the information you need.
- Establishing a technical report.

Procedures that Cyber Forensic Experts Follow:

Identification: The first step of cyber forensics experts is to identify what evidence is present, where it is stored, and in which format it is stored.

Preservation: After identifying the data, the next step is to safely preserve the data and not allow other people to use that device so that no one can tamper data.

Analysis: After getting the data, the next step is to analyze the data or system. Here the expert recovers the deleted files and verifies the recovered data and finds the evidence that the criminal tried to erase by deleting secret files. This process might take several iterations to reach the final conclusion.

Documentation: Now after analyzing data, a record is created. This record contains all the recovered and available(not deleted) data which helps in recreating the crime scene and reviewing it.

Presentation: This is the final step in which the analyzed data is presented in front of the court to solve cases.

Types of computer forensics

Network forensics:

This involves monitoring and analyzing the network traffic to and from the criminal's network. The tools used here are network intrusion detection systems and other automated tools.

Email forensics:

In this type of forensics, the experts check the email of the criminal and recover deleted email threads to extract out crucial information related to the case.

Malware forensics:

This branch of forensics involves hacking related crimes. Here, the forensics expert examines the malware like trojans to identify the hacker involved behind this.

Memory forensics: This branch of forensics deals with collecting data from the memory(like cache, RAM, etc.) in raw and then retrieve information from that data.

Mobile Phone forensics:

This branch of forensics generally deals with mobile phones. They examine and analyze data from the mobile phone.

Database forensics:

This branch of forensics examines and analyzes the data from databases and their related metadata.

Disk forensics:

This branch of forensics extracts data from storage media by searching modified, active, or deleted files.

Techniques used for cyber forensics

Reverse steganography:

Steganography is a method of hiding important data inside the digital file, image, etc. So, cyber forensic experts do reverse steganography to analyze the data and find a relation with the case.

Stochastic forensics:

In Stochastic forensics, the experts analyze and reconstruct digital activity without using digital artifacts. Here, artifacts mean unintended alterations of data that occur from digital processes.

Cross-drive analysis:

In this process, the information found on multiple computer drives is correlated and cross-references to analyze and preserve information that is relevant to the investigation.

Live analysis:

In this technique, the computer of criminals is analyzed from within the OS in running mode. It aims at the volatile data of RAM to get some valuable information.

Deleted file recovery:

This includes searching for memory to find fragments of a partially deleted file in order to recover it for evidence purposes.

Advantages

- Cyber forensics ensures the integrity of the computer.

- Through cyber forensics, many people, companies, etc get to know about such crimes, thus taking proper measures to avoid them.
- Cyber forensics find evidence from digital devices and then present them in court, which can lead to the punishment of the culprit.
- They efficiently track down the culprit anywhere in the world.
- They help people or organizations to protect their money and time.
- The relevant data can be made trending and be used in making the public aware of it.

Skills Required for a Cyber Forensic Investigator

- As we know, cyber forensic based on technology. So, knowledge of various technologies, computers, mobile phones, network hacks, security breaches, etc. is required.
- The expert should be very attentive while examining a large amount of data to identify proof/evidence.
- The expert must be aware of criminal laws, a criminal investigation, etc.
- As we know, technology always changes over time, so the experts must be updated with the latest technology.
- Cyber forensic experts must be able to analyse the data, derive conclusions from it and make proper interpretations.
- The communication skill of the expert must be good so that while presenting evidence in front of the court, everyone understands each detail with clarity.
- The expert must have strong knowledge of basic cyber security.

Firewall & its Settings

A firewall can be defined as a special type of network security device or a software program that monitors and filters incoming and outgoing network traffic based on a defined set of security rules. It acts as a barrier between internal private networks and external sources (such as the public Internet), shown in Figure 3.1.

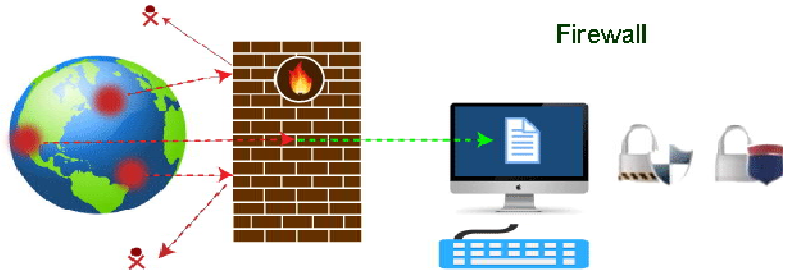

Figure 3.1 Firewall

The primary purpose of a firewall is to allow non-threatening traffic and prevent malicious or unwanted data traffic for protecting the computer from viruses and attacks. A firewall is a cybersecurity tool that filters network traffic and helps users in blocking malicious software from accessing the Internet in infected computers. Firewall can be implemented as a hardware or a software. Each format has different functionality but for the same purpose. A hardware firewall is a physical device that attaches between a computer network and a gateway. eg. a broadband router. On the other hand, a software firewall is a simple program installed on a computer that works through port numbers and other installed software. An illustration of Firewall is shown in Figure 3.2.

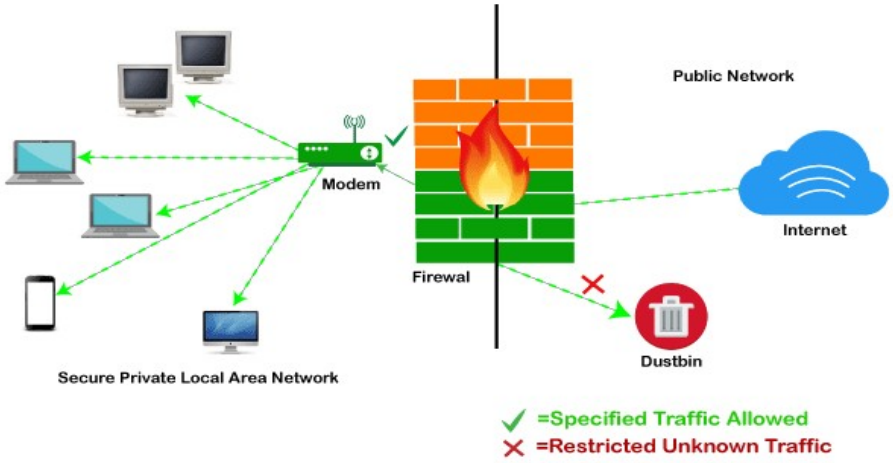

Figure 3.2 Illustration of Firewall

Need for a Firewall:

- Open Access: Without a firewall, we make our devices vulnerable to malicious users and other unwanted sources.
- Lost or Comprised Data: In this case, cybercriminals can easily delete our data or use our personal information for their benefit.
- Network Crashes: In the absence of a firewall, anyone could access our network and shut it down.

Evolution of Firewall:

Firewalls have existed since the late 1980's and started out as packet filters. Firewalls have come a long way as technologies developed throughout the decades.

Gen 1 Virus: Generation 1, Late 1980's, virus attacks on stand-alone PC's affected all businesses and drove anti-virus products.

Gen 2 Networks: Generation 2, Mid 1990's, attacks from the internet affected all business and drove creation of the firewall.

Gen 3 Applications: Generation 3, Early 2000's, exploiting vulnerabilities in applications which affected most businesses and drove Intrusion Prevention Systems Products (IPS).

Gen 4 Payload: Generation 4, Approx. 2010, rise of targeted, unknown, evasive, polymorphic attacks which affected most businesses and drove anti-bot and sandboxing products. Sandboxing is a cybersecurity practice where you run code, observe and analyze and code in a safe, isolated environment on a network that mimics end-user operating environments.

Gen 5 Mega: Generation 5, Approx. 2017, large scale, multi-vector, mega attacks using advance attack tools and is driving advance threat prevention solutions.

Today's firewalls, including Next Generation Firewalls and Network Firewalls support a wide variety of functions and capabilities with built-in features, including: Network Threat Prevention, Application and Identity-Based Control, Hybrid Cloud Support, Scalable Performance, Network traffic management and control, Access validation and Record and Report on Events.

Limitations of Firewall:

- Firewalls cannot stop users from accessing malicious websites, making it vulnerable to internal threats or attacks.
- Firewalls cannot protect against the transfer of virus-infected files or software.
- Firewalls cannot prevent misuse of passwords.

- Firewalls cannot protect if security rules are misconfigured.
- Firewalls cannot protect against non-technical security risks, such as social engineering. (Examples of social engineering threats include malicious device drops (usb attacks) and convincing users to divulge sensitive information using either in-person or digital forms of communication.)
- Firewalls cannot stop or prevent attackers with modems from dialing in to or out of the internal network.
- Firewalls cannot secure the system which is already infected.

Types of Firewall

Depending on their structure and functionality, there are different types of firewalls. The following is a list of some common types of firewalls:

Proxy Firewall:

Proxy firewalls operate at the application layer as an intermediate device to filter incoming traffic between two end systems (e.g., network and traffic systems). Also called as 'Application-level Gateways'.

Packet-filtering firewalls:

It is the most basic type of firewall. It acts like a management program that monitors network traffic and filters incoming packets based on configured security rules.

Stateful Multi-layer Inspection (SMLI) Firewall:

It includes both packet inspection technology and TCP handshake verification. It also keeps track of the status of established connections.

Unified Threat Management (UTM) Firewalls:

It is a special type of device that includes features of a stateful inspection firewall with anti-virus and intrusion prevention support.

Next-generation firewall (NGFW):

It is the latest released firewalls are usually defined as 'next-generation firewalls'. as a security device combining the features and functionalities of other firewalls. These firewalls include deep-packet inspection (DPI), surface-level packet inspection, and TCP handshake testing, etc.

Network address translation (NAT) firewalls:

It is primarily designed to access Internet traffic and block all unwanted connections. These types of firewalls usually hide the IP addresses of our devices, making it safe from attackers. Works like a proxy firewall.

Cloud Firewall:

It is typically maintained and run on the Internet by third-party vendors. Similar to proxy firewall. Also known as FaaS (Firewall-as-a-Service)

Firewall settings or Firewall configuration

A firewall plays a vital role in network security and needs to be properly configured to keep organizations protected from data leakage and cyberattacks.This is possible by configuring domain names and Internet Protocol (IP) addresses to keep the firewall secure. Firewall policy configuration is based on network type, such as public or private, and can be set up with security rules that block or allow access to prevent potential attacks from hackers or malware. The default settings on most firewalls and protocols like the File Transfer Protocol (FTP) do not provide the necessary level of protection to keep networks secure from cyberattacks. Organizations must ensure basic firewall configuration meets the unique needs of their networks.

Steps to configure a firewall securely:

Secure the Firewall:

Securing a firewall is the vital first step to ensure only authorized administrators have access to it. This includes actions such as:

- Update with the latest firmware
- Never put firewalls into protection without appropriate configurations in place
- Deleting, disabling, or renaming default accounts and changing default passwords
- Use unique and secure passwords
- Never use shared user accounts. If a firewall will be managed by multiple administrators, additional admin accounts must have limited privileges based on individual responsibilities
- Disabling the Simple Network Management Protocol (SNMP), which collects and organizes information about devices on IP networks, or configuring it for secure usage
- Restricting outgoing and incoming network traffic for specific applications or the Transmission Control Protocol (TCP)

Establish Firewall Zones and an IP Address Structure:

It is important to identify network assets and resources that must be protected. This includes creating a structure that groups corporate assets into zones based on similar functions and the level of risk.

A good example of this is servers such as email servers, virtual private network (VPN) servers, and web servers placed in a dedicated zone that limits inbound internet traffic, often referred to as a demilitarized zone (DMZ). A general rule is that the more zones created, the more secure the network is.

However, having more zones also demands more time to manage them. With a network zone structure established, it is also important to establish a corresponding IP address structure that assigns zones to firewall interfaces and subinterfaces.

Configure Access Control Lists (ACLs):

Access control lists (ACLs) enable organizations to determine which traffic is allowed to flow in and out of each zone. ACLs act as firewall rules, which organizations can apply to each firewall interface and subinterface.

ACLs must be made specific to the exact source and destination port numbers and IP addresses. Each ACL should have a “deny all” rule created at the end of it, which enables organizations to filter out unapproved traffic.

Each interface and subinterface also needs an inbound and outbound ACL to ensure only approved traffic can reach each zone. It is also advisable to disable firewall administration interfaces from public access to protect the configuration and disable unencrypted firewall management protocols.

Configure Other Firewall Services and Logging:

Some firewalls can be configured to support other services, such as a Dynamic Host Configuration Protocol (DHCP) server, intrusion prevention system (IPS), and Network Time Protocol (NTP) server. It is important to also disable the extra services that will not be used. Further, firewalls must be configured to report to a logging service to comply with and fulfill Payment Card Industry Data Security Standard (PCI DSS) requirements.

Test the Firewall Configuration:

With the configurations made, it is critical to test them to ensure that the firewall performs as intended. The configuration can be tested through techniques like

penetration testing and vulnerability scanning. It is essential to back up the configuration in a secure location in case of any failures during the testing process.

Manage Firewall Continually:

Firewall management and monitoring are critical to ensuring that the firewall continues to function as intended. This includes monitoring logs, performing vulnerability scans, and regularly reviewing rules. It is also important to document processes and manage the configuration continually and diligently to ensure ongoing protection of the network.

Mistakes To Avoid When Setting Up a Firewall:

Configuring a firewall can present difficulties, which can commonly be prevented by avoiding common mistakes, such as:

- Using broad policies or the wrong firewall settings can result in server issues, such as Domain Name System (DNS) and connectivity issues.
- Ignoring outgoing traffic can present a risk to networks.
- Relying solely on a firewall for network security or non-standard authentication methods may not protect all corporate resources.

Different measures to protect against cyber fraud

Continually Update Your Computer and Mobile Devices:

Cybercriminals frequently gain access to information by using known flaws in the software and operating systems that run your computer or phone.

Updates are crucial; patching these flaws and vulnerabilities can make it less likely that you will become a victim of a successful cyberattack.

Employ Antivirus Software and Anti-malware Protection on Your Computers:

Cybercriminals also use technical attacks to deploy viruses, botnets, malware, keyloggers and spyware to infect or take over your machine.

Make sure the software solutions you choose provide adequate protection, keep them updated with the latest virus definitions and schedule full scans to run at least once per week.

Use Good Password Habits:

Change your passwords every three to six months, create strong passwords that are difficult to guess, and do not repeat passwords across multiple websites.

Remember to use a combination of letters, numbers and symbols whenever possible.

Strengthen Your Home Network:

It may seem daunting to actively manage all your devices, but starting with your internet router will improve your security at the source. Change the password from the default provided by your ISP, and choose the appropriate encryption.

Access to your computer and devices:

For mobile devices, enable a PIN/passcode and choose the option within your settings for auto-lock. For computers, keep multiple profiles, which will enable you to apply restrictions to accounts used by younger children.

Back Up the Data on Your Computer and Your Mobile Devices:

Even the best machine or device may become compromised or crash. Regular backups to an external hard drive will help you recover your information in these situations.

Awareness to all users about internet security:

Young children are vulnerable to even the most basic of cyber tricks. Teenagers are in online more frequently and often visit riskier sites, such as file

sharing platforms for movies, videos and games. Elder people often have what every criminal wants: financial assets and limited digital knowledge.

Understand and Protect Against Identity Theft:

Certain types of personal information can be used to commit fraud, such as account takeovers, unauthorized money transfers or new lines of credit opened in your name.

One can protect against identity theft by shredding sensitive documents, avoiding suspicious links and attachments in your email, learning to recognize and block smishing attacks.

Know What To Do If You Become a Victim:

If you discover that your information has been exposed, you may want to enable a fraud alert or a credit freeze on your credit information.

Keep Control of Your Information:

Do not automatically hand over social security numbers, account numbers or other highly sensitive information just because you are asked. Also, never release your credit or debit card information to someone who initiates contact with you.

Cyber Netiquette

Netiquette is a made-up of the words net and etiquette. Netiquette thus describes the rules of conduct for respectful and appropriate communication on the internet. Netiquette is often referred to as etiquette for the internet. These are not legally binding rules, but recommended rules of etiquette. Cyber netiquette, also known as internet etiquette, refers to the rules of behavior and courtesy that individuals should follow when interacting online. These guidelines help to ensure that online communication is respectful, effective, and productive. When communicating on the internet, you should always remember that you are communicating with people and not simply with computers or smartphones.

Netiquette: General rules of conduct:

There are 20 general recommendations for conduct on the internet that to be followed when communicating online. They are as follows:

Stick to the rules of conduct online that you follow in real life:

When communicating online, refrain from insulting, provoking, threatening or insulting others. Respect the opinions of your chat counterparts and express constructive criticism.

Think of the person:

Think of the person behind the computer when you compose your messages. You are not communicating with a machine, but with real people. Also, consider what and how you write. Because a screenshot or a copy of your messages is quickly made in the internet and still exists even if you delete your messages afterward.

Present your best side online:

Communication on the internet comes with a certain anonymity that does not exist in real life when you are talking to someone face to face. Often this anonymity leads to a lower inhibition threshold for many users and they behave rudely online. Make sure that you show your best side online. Good netiquette is characterized by respect, politeness and professionalism.

Read first, then ask:

Remember that conversations online can happen very quickly. It is therefore important to gather all the information before responding or asking questions.

Pay attention to grammar and punctuation:

Check them for grammar, punctuation and correct spelling. It can be very frustrating for the other person if they have to decode poorly written sentences. Faulty grammar also distracts from the goal of your message. If you have a weakness in grammar and spelling, use spelling aids before you send messages.

Respect the privacy of others:

This rule should be followed not only in everyday use of online communication, but also at work. Do not simply forward information that has been sent to you without first obtaining permission from the original sender. When sending private emails to multiple recipients, use BCC (blind carbon copy) instead of CC (carbon copy). Many people do not like their names and email addresses being passed on to people they do not know themselves. This rule on the internet also applies to uploading and sharing photos or videos that show other people.

Respect the time and bandwidth of others:

Today we are living in the fast internet world. Information can be sent to different people around the world in a matter of seconds. But you should think of limited receptivity of information when you send messages to your friends, colleagues or superiors. No one wants to waste time unnecessarily on an email where core message is only at the end of the email. It consumes time and effort and is simply annoying.

Forgive the mistakes of others:

In online communication, always a beginner can make mistakes. Often these are spelling mistakes, superfluous questions or answers that are too long. These can be a lack of etiquette or manners. It's important to forgive your counterparts' mistakes in case of minor mistakes. If you want to express sarcasm among friends or close colleagues, use emojis such as smileys or GIFs.

Don't abuse your power:

On the internet, as in real life, some people have more power than others. Examples are Moderators in a forum, experts in companies or system administrators. If you have more power than others, you do not have the right to exploit this power. For example, system administrators should never read private emails in the company.

Help keep flame wars under control:

Flame wars are messages that contain aggressive personal criticism or attacks on a person. In group chats, heated discussions often degenerate into so-called flame wars. Always remember that you should treat others as you would like to be treated. Profanity (Bad language) is not part of netiquette.

Know where you are in cyberspace:

Netiquette is interpreted differently in different places on the internet. For example, it is perfectly normal to spread gossip in a TV discussion group. However, if you do this in a serious discussion group, you will quickly make yourself unpopular. if you are in a new area that is unfamiliar to you, you need to look around and learn the ropes. Get an idea of how other people in this area of cyberspace communicate with each other and adapt to them.

Hate speech and netiquette:

Hate speech on the internet is an increasing problem, especially in social media. It is often found in offensive comments under photos or posts. If you come across such statements on the internet, you should report them to the provider of the website.

Children on the internet: Do not give out personal information

In these times of social media, identity theft and social engineering, keeping personal information secret is essential. Under no circumstances should your child share passwords or personal information such as their name, address or telephone number online. The name of the school should also be kept secret.

Use a neutral nickname:

Under no circumstances reveal your child's identity. Make sure that your child uses a neutral nickname in chat rooms.

Netiquette and bots/troll posts:

Bots are computer programs that automatically follow up on a task without requiring any interaction with humans. They often spam in forums or in the comments under posts. This is annoying and time-consuming, as these responses have to be identified and removed. Bots are therefore not part of netiquette and should be avoided if at all possible.

Rules for children on the internet: Do not trust chat participants:

You never know who is really hiding behind the funny profile name and picture. For example, your child should never meet a stranger just because they got along well in a chat conversation. It could be an adult with bad intentions. Similarly, you should explain to your child that they should not add strangers as friends on social media such as Facebook or Instagram.

Fairness first: Do not exclude anyone:

If your child is communicating in a private group, chat participants should not feel excluded. Netiquette includes values such as tolerance, respect and helpfulness. This also means that only the language used by everyone should be used. In a school group chat, your child should always make sure that all chat members are on the same level.

Netiquette for children: Keep it short and clear

Posts, answers and even questions should be kept as short and clear as possible. No one wants to read an unnecessary amount of text that does not contribute to answering the issue.

Netiquette and online learning:

During COVID-19 pandemic, most teaching in schools was done online. In the online teaching,

- Children should support one another
- Children not to take screenshots of lessons without the teacher's permission.
- Passwords and credentials given by the school must not be passed on by children to third parties.
- Children should be ready a few minutes before class starts.
- Pupils should speak up if they have any questions or comments.

Trust your child:

Trust in your offspring's abilities, and refrain from constantly monitoring their internet activities. It is usually enough to know that your child can ask you for help if the worst happens.

If you follow the above rules of netiquette, you will have no problems with online communication in everyday life, in class or at work. In addition, your respectful and friendly behavior will be noticed positively by your colleagues and superiors. Especially for children, it is important to learn the correct rules of etiquette on the internet at an early age. Social interaction and the correct rules of etiquette and behavior on the internet are just as important as in real life.

Cyber Netiquette onboard

In response to the growing threat of cyber crime, the International Maritime Organization (IMO) has issued Resolution MSC.428(98). On January 1, 2021, IMO Resolution MSC.428(98) came into force. This regulation is applicable to all vessels, requiring ships to include cyber risk management in their safety management systems, in accordance with the International Safety Management (ISM) Code. This resolution further encourages flag administrations to ensure that ship owners and managers are properly addressing cyber risks.

Cybersecurity onboard a ship is essential to protect the ship's information and communication systems from unauthorized access, theft, or damage. In addition to implementing technical measures such as firewalls, antivirus software, and encryption protocols, practicing good cyber netiquettes is also important for ensuring the safety and security of onboard systems.

Here are some cyber netiquettes that can help enhance cybersecurity on board a ship:

Use strong passwords: Crew members should use strong and unique passwords for all their accounts and devices. A strong password should include a combination of upper and lowercase letters, numbers, and symbols. Passwords should also be changed regularly.

Beware of phishing scams: Phishing scams are designed to trick individuals into revealing sensitive information such as login credentials, credit card numbers, and personal details. Crew members should be cautious of suspicious emails or messages and should not click on links or download attachments from unknown sources.

Secure devices: All onboard devices should be secured with antivirus software, firewalls, and encryption protocols. This will help protect against malware and other cyber threats.

Use secure Wi-Fi connections: When connecting to the ship's Wi-Fi network, crew members should ensure that they are using a secure connection that is encrypted. They should also avoid using public Wi-Fi networks that may not be secure.

Limit access to sensitive information: Crew members should only have access to information that is necessary for their job. Access to sensitive information should be restricted to authorized personnel only.

Report suspicious activity: If crew members notice any suspicious activity or cyber threats, they should report it immediately to the ship's IT department or captain.

By practicing these cyber netiquettes, crew members can help enhance cybersecurity on board a ship and protect against cyber threats.

Relevant Video links:

1. https://www.youtube.com/watch?v=1Luh3tBH-8I
2. https://www.youtube.com/watch?v=qS4ViqnjkC8
3. https://www.youtube.com/watch?v=ln4KTJLFV4U
4. https://www.youtube.com/watch?v=5juUB09V9E8
5. https://www.youtube.com/watch?v=inWWhr5tnEA

References:

1. https://www.javatpoint.com/cyber-security-tutorial
2. https://knilt.arcc.albany.edu/images/b/b3/Unit4_LectureNotes.pdf
3. https://www.javatpoint.com/ethical-hacking
4. https://www.geeksforgeeks.org/different-types-of-websites/
5. https://www.mygreatlearning.com/blog/cybersecurity-vulnerabilities/
6. Beissel, S. (2016). Cybersecurity Safeguards. In: Cybersecurity Investments. Progress in IS. Springer, Cham. https://doi.org/10.1007/978-3-319-30460-1_3
7. https://www.javatpoint.com/ips-intrusion-prevention-system
8. https://www.techtarget.com/searchsecurity/definition/intrusion-detection-system
9. https://www.vedantu.com/commerce/introduction-to-cyberspace
10. https://www.geeksforgeeks.org/cyber-forensics/
11. https://www.javatpoint.com/firewall
12. https://www.fortinet.com/resources/cyberglossary/firewall-configuration
13. https://www.kaspersky.com/resource-center/preemptive-safety/what-is-netiquette