What is cybersecurity?

It is defined as the set of preventive measures taken to protect an individual's or an organization's computer system from unauthorized digital access. The foundation of protecting information is known as the CIA triad which stands for confidentiality, integrity, and availability. Confidentiality is the need to impose access to information only to certain individuals, integrity ensures that data is maintained so it is not altered or deleted, and availability is securing data so that it is timely and reliably available for users to access.

The cybersecurity domains

To put it simply, domains are different areas in the cybersecurity field. These include information security, network security,application security, cryptography, risk management and so on.

Security standards, regulations, and frameworks

Measures that support cybersecurity from the potential consequences of digital crimes

Standards are security guidelines that form the basis of security maintenance for organizations. They are usually imposed recommendations.
Regulations are laws enforced by the government that organizations must follow to ensure overall security protection.
Frameworks are a set of practices, standards, and guidelines that provide strategies for organizations to mitigate digital attacks.

Cybercrime

A criminal activity which targets a computer or a computer system. Cybercrimes include fraud, theft, phishing scams, and many more.

Digital forensics

A branch of cybersecurity responsible for the investigation of devices that store digital data. It is the process of identifying, securing, analyzing, and documenting digital evidence to be presented in the court of law. It encompasses a wide range of fields including disk forensics, network forensics, memory forensics, mobile forensics, and cloud forensics.

Malware

A malicious intrusive software used by cyberattackers to gain unauthorized access to a computer system.
Some examples of malware are:
Viruses
Adware
Spyware
Scareware
Trojan horses
Rootkits
Ransomware
Worms
Fileless malware

1)Virus

It is a malware which attaches itself to a host found on a computer system. A virus requires user activation in order to alter or delete information and data held on one's computer.

2)Adware

It is an intrusive software which displays advertisements. Although not as dangerous as other malware despite posing several risks, adware is usually more annoying.

3)Spyware

It is a violating malicious software which is downloaded on a computer system with the intent of gathering private information and relaying it to another individual or organization. Sometimes, a spyware may contain a keylogger which records everything a victim types into their computer.

4)Scareware

It is a form of malware which attempts to frighten users by claiming there's an issue with their computer system. Usually, it takes the form of pop-up ads from alleged cybersecurity organizations.

5)Ransomware

It is a type of permanent malware which encrypts data or information, rendering them inaccessible for users. Cyber criminals will then demand ransom in return for decryption.

6)Fileless malware

It is a usually hard-to- detect type of malware as it directly operates within a legitimate software installed on your computer system. This malicious code doesn't use your hard drive to damage your computer. Instead, it works on your operating system.

7)Worms

Unlike viruses, worms are self-replicating malware that don't need user intervention to damage a computer. After overloading a system, a worm is capable of violating availability.

8)Trojan

It is a non-trustworthy malware which disguises itself as an actual anti-security program to guide users to download it and eventually provide access for hackers and scammers.

Further example of a malware:

Sometimes, a trojan may be used to grant cyber criminals remote third-party access to a computer system. The intent behind this rootkit may have been ransomware which prevents victims from accessing their data and information.

Suggestions against Malware:

Install trustworthy antivirus software
Avoid clicking on suspicious links and ads
Regularly backup your computer
Use an ad-blocker
Choose strong passwords

Cyberattacks

Phishing:

It is a social engineering practice which uses human interactions made via texts or calls to obtain personal information or to install malware. There are many types of this cyberattack which relies on communication such as spear phishing, vishing, smishing, and whaling.

Aside from that, a cyber attacker may resort to other methods to harm a computer system by secretly embedding malicious code. For example, an attacker may hide a malicious code in a seemingly safe document, attach it to an email which is then sent to an individual, and then trick the user to open it and execute it.

Email spoofing:
It is a cyber security attack which relies on an attacker's disguise as a genuine sender. Attackers use this method to manipulate organizations into thinking they are a trusted source in order to achieve their desired goals.

SQL Database
Short for structured query language, SQL is a programming language used to manage and interact with data stored in SQL database systems. For most web applications, it is most commonly used to structure and maintain relational data. SQL works through command statements that alter data.
E.g: Select, Insert, Update.....

What are SQL injections?
It is when an attacker injects code via user input to interfere with queries inside a database. By using the following methods, attackers gain access to precious data which allows them to change records and control a system.

Union-based injections
In a union-based injection, attackers may combine the results of two SELECT statements to gather data from two separate relational database tables.
Error-based injections
It is a technique by which the attacker inserts a query to force the application to extract data and to give information about the structure of the database.
Boolean-based injections
This technique relies on statements that force the application to confirm whether they're true or false which helps the attacker know more about the database.
Time-based injections

This type of injection relies on delays for statement responses which can help the attacker infer information about the database.

Out-of-band SQL injections

Rare type of injections as they are harder to execute.

How to prevent SQL injections

Sanitization : It means that you remove potentially harmful characters from input by assessing everything which goes into the database.

Web attacks: XSS and CSRF

Cross- Site scripting is a type of security attack where a hacker injects unsanitized input (code) into a browser. Usually, the attacker may be able to redirect users to malicious pages and to steal information and data. There are three major types of this malicious web attack.

Stored XSS:

This happens when a web browser or page saves the malicious input an attacker may have just inserted. After clicking on the code, the server executes it on the user’s computer.

Reflected XSS:

This occurs when a malicious script is injected into trustworthy websites and then reflected into a user’s browser. After being executed, the script returns to the attacker with the user’s information.

DOM-based XSS:

A document object model is a programming interface which allows for manipulation of data. That is to change the structure, style, and content of a web page document by a program. A DOM-based attack merely modifies a user’s browser and not the server itself. By manipulating the user’s browser, an attacker can inject malicious code.

These types of attacks can be prevented by removing dangerous characters such as <, >, ", =.

Cross-site Request Forgery

Another type of security attack which happens when session controls and management aren't properly handled. For example, a user may request from an application to change their password. When active user sessions are managed in a flawed manner, an attacker is able to input requests and change a user's password which would allow control over a victim's account.

This attack can be handled by CSRF token values which verify whether an account belongs to a user or not. For example, a user may be asked to write their current password to verify whether they're an attacker in disguise.

Zero-day attacks

A zero-day attack is a threat which enterprises must be aware of and prepared to handle in case of occurrence. Basically, it is a software bug by which an attacker takes advantage of a flawed security system to gain unauthorized access, steal information and data, or simply insert malicious code. This type of attack can go undetected for months and even years which makes it hard to mitigate.

DDoS

It is when an attacker overloads a system and causes it to crash. An attacker would make multiple requests using multiple resources (computers) to overwhelm a system and eventually take it down. So, where does the attacker get all these computers from? To put it simply, websites are prepared to handle several requests on a daily basis. By infecting Botnet malware to countless devices, an attacker is able to cause non-manageable web traffic. These types of attacks are perpetrated by attacking different network layers by which 3 of the 7 different layers are differently attacked.

This attack can be avoided by limiting the number of requests at a single time. CAPTCHAS can also be used as they verify whether users are humans or bots in an attempt to only allow actual traffic to log in.

Cryptography

It is basically encrypting or decrypting data which allows for communication and exchange between servers and users while ensuring safe transmission. Encrypting is hiding encoded data while decrypting is revealing it.

Asymmetric vs Symmetric Encryption

The first one uses two different keys to encrypt and decrypt data while the second one uses the same key. Asymmetric encryption is far more reliable and safer to use as it provides senders with two keys: a private one and a public one. The public one is used to encrypt data and is usually granted for recipients to allow the transmission of messages while the private one remains only known by the sender for the decryption of data. If you would like to send a message back to the recipient, they would have to provide you access to their public key.

How do computers encrypt and decrypt using XOR?

To elaborate, XOR is an operation which performs logical operators and returns a value of the two bits compared.

Hashing

It is a process by which data is hashed using mathematical functions to learn whether it has been altered or not. While every hash should generate a unique function, two different inputs can generate the same input.
Hashes are commonly used to protect data. One example of this would be using the functions of passwords to store them in a database. In case of breaching, a hacker would not be able to view passwords.

Rainbow tables

Although hash functions can't be encrypted or decrypted by hackers, it is still possible for them to use massive password tables to break into the database and gain access to accounts after viewing passwords.

Salts

By using a secret random string-also known as salts- organizations can ensure security of their hashing information by combining a complex password with salts.

Authentication and Authorization

Authentication is the verification of who you are and Authorization is the verification of what you have the right to do.The former is related to finding out about a user's identity while the latter ensures access only to authorized content and information for the user. The more methods of authentication used, the safer one's assets are. This is rather known as multi-factor authentication.

How are users given access by a website after logging in?

Data between users and a server is communicated by the website server's API which receives and sends data. There are three main types of API authentication

1) HTTP Basic Auth

It is a very simple and basic way of communication as users are only asked to provide their usernames and passwords when they log in to a website. Usually, this isn't needed if you have cookies turned on as they save your credentials so you don't have to provide them each and every time.

2)API Keys

Unlike HTTP basic auth, API keys are complex unique strings of random numbers and letters generated for each user.

3)Oauth

A practical method by which users can log in to a website using Google and many other websites. Users are then redirected to another web page to authenticate themselves. The website will then send a password to verify the identity of users.

Role-based access control

This is a concept by which users are granted permission to certain things based on their roles.

Basic networking

How do users interact on the internet? How do they access websites and web pages? Networking enables devices to gain access to content and communicate together. A network is basically two or more devices connected together. These networks happen to rely on standards that have been built decades ago to guide security professionals

Types of networks

1) LAN

A local area network consists of multiple devices connected in a limited space.

2) CAN

A campus area network involves the connection of several devices over a large area.

3) WAN

A wide network area usually connects devices from different geographical areas.

OSI (Open System Interconnection)

It is a conceptual model which divides networks into seven different layers based on their specific roles. Each layer interacts with the one prior to it and provides information for the one after it.

Layer one: Physical

A concrete example of this layer would be a physical medium such as wires which allow bits to transfer through them. This layer includes hardware parts. The line configuration of the physical layer decides how two devices can be connected using wires. Further, it defines data transmission between two devices, the type of signals used, and how these network devices are arranged. Technologies such as wifi, bluetooth, and ethernet cables are mere examples.

Layer 2: Data-Link

This layer is responsible for many tasks including providing safe communication between two devices, structuring data into frames, identifying each and every device using their 48 unique bits, and detecting errors within data frames. Data frames and Media Access Control (MAC) addresses are mere examples.

Layer 3: Network
This layer determines the way data packets move from their source to their destination within the internet (a wide network). While the second layer ensures the transmission of data frames using MAC addresses over local area networks, the network layer describes how data packets go from an IP address to another IP address. Each computer is assigned to a unique IP.

Layer 4: Transport
This layer applies to the actual transfer of data. It ensures that data is fully transmitted with no errors after segmentation.

Layer 5: Session
This layer is responsible for session management which refers to the exchange of information between two devices. Authentication and authorization when a user tries to log into a website is an example of session management.

Layer 6: Presentation
This layer changes data into formats by which applications can display and make usable for users.

Layer 7: Application
It consists of websites, web pages, and mobile applications which make use of internet data so that users can view their content.

TCP/IP model
Aside from the OSI model, there's also the IP model which describes networking in four different layers.

Application layer which refers to the interactions between content of an application and users. Here, there are multiple protocols including HTTP, FTP, SMTP, and more.
Transport layer which ensures flow control and error recovery between a sender and a recipient. It encompasses two main protocols: the TCP and UDP.
Internet layer which is responsible for addressing and routing data.

Network access layer which combines the two layers of the OSI model (the physical and data-link). It encompasses the physical medium for data transmission between two devices.

Network protocols
They are basically a set of standards which form the basis for the exchange of information between devices to ensure safe and easy transmissions. To understand network protocols better, it is recommended to think of them as languages but to computers. To put it simply,these protocols govern communications between devices. There are several protocols which belong to the various OSI layers as well as the TCP/IP model. A common protocol example to ensure one understands this concept would be IP addresses. As mentioned before, each computer is marked by a unique IP address made up of four numbers from 0 till 255 which allows us to differentiate between each and every PC. To successfully reach their target, data packets must know the IP address of their recipient. The protocol for IP addresses is known as the Internet protocol.

How do they exactly work?
Network protocols break down large tasks into smaller ones across different layers of the network to facilitate data communication and ensure it is done in a safe manner.

The primary actions of network protocols
There are myriads of network protocols, but their target actions boil down to three and they are:
Communications which include automation, instant messaging, routing, bluetooth transfer, and even the internet protocol.
Network management which includes connection, link aggregation, and troubleshooting.
Security which includes transportation, authentication, and encryption.

Most common examples of internet protocols:

DNS (Domain name system)
This protocol converts domain names into IP addresses. Since every host is identified by its IP address which would be hard to remember,

users request the URL for a website which is sent to a DNS server by one's computer.

HTTP (Hypertext transfer protocol)

This defines the process by which web browsers respond to requests and commands such as GET, POST, PUT, and HEAD.

SSH (Secure shell)

A protocol which allows system administrators to safely access a remote computer or virtual machine even when using insecure internet.

FTP (file transfer protocol)

It enables the transfer of files from one host to another using the internet or between computer systems.

Firewalls

It is a cybersecurity tool which inspects incoming and outgoing data packets. It's basically a barrier which differs depending on the device we aim to protect. What a firewall accepts or denies from entering a secure network environment merely depends on the rules we set which may range from the IP address of a packet3, its contents, or the details of its network sessions.

Types of firewalls:

Packet-filtering firewalls

These firewalls work at the network layer and inspect information such as source IP, destination IP, and the flow of data packets within a network.

Circuit-level firewalls

These firewalls manage and review individual sessions to validate data packets and identify if they're from a legitimate source.

Stateful-inspection firewalls

These firewalls monitor active user sessions by maintaining a table consisting of these session details. They are basically responsible for ensuring the content of data packets is safe. They are found in the layers 3 and 4 of the OSI model.

Application firewalls:
These firewalls offer a specialized layer of security for applications as they operate within layer 7 of the OSI. They safeguard applications from cross-site scripting and SQL injections. Although an HTTP request may appear as safe to pass, this firewall can inspect its content for potentially harmful and malicious data.

Next-generation level firewalls:
Unlike traditional firewalls, next-generation ones are more advanced and complex as they offer a high level of security protection against sophisticated modern threats. NGFWs typically employ AI, rendering them a bit more costly.

How are firewalls rules set?
A system administrator of an organization may set certain actions for a firewall such as forward which allows the packet to go in and drop which inhibits its entrance. As for IP sources and destination, you would have to use a wildcard value such as x.x.x.x which would allow all packets to go in. Ports are standardized layer 4 models which allow devices to distinguish between different types of traffic. Only the protocols UDP and TCP can indicate where a packet should go.

Wireless network security
With the rise of Wi-Fi usage, there must exist prevention methods to avoid the dangers of unauthorized network access.

Network segmentation
It is the process of turning large networks into smaller ones with different access levels which would improve overall security for large corporations and organizations. To do so, we must determine which assets we're trying to protect and which individuals can access these assets.

Access point placement

They are basically the systems used to distribute wireless signals. Putting them in easily accessible places makes them vulnerable to attackers who would place users at risk.

Encryption

The current common standard for wireless security is WPA2. The personal one requires a single password while the enterprise one requires multi-factor authentication. It is often recommended to set up one's own password for Wi-Fi instead of using the one found on the router.

Network monitoring

Personal security

Every individual born in the modern era and is a part of the digital world is at risk of cyber attacks and crimes. As computers play a vital role in our every-day lives, they have become a critical target for hackers to gain access to for their own advantage. Hence, there are several methods one can employ to ensure that his/her personal device isn't put at risk. To stay safe while surfing online, one should choose secure and legit tools and stay up to date with the latest cyber knowledge and systems. These are some of the best actions you can do to harden your device.

Account safety

Reusing passwords

Each and every account requires a password. More often than not, some individuals may reuse the same password for several accounts. While it may be sort of hard to guess a password, there are several methods attackers may employ such as brute-forcing, credential stuffing, dictionary attacks, and rainbow tables. Furthermore, considering the fact that hundreds of websites are hacked everyday, reusing the same passwords puts users at risk as hackers would try to use them on other sites and gain access over one's account.
Visit this website to ensure that your password is secure:
https://www.security.org/how-secure-is-my-password/
To find out whether your email address has been involved in a data breach, consider visiting the following site

https://haveibeenpwned.com/

Password manager
It is a software in a browser that comes in an extension form. It saves all your passwords in an encrypted form in case you ever forget them. You only have to remember one password and that is the master one. The master password allows you to access and decrypt all of your passcodes.

Multi-factor authentication
Always make sure to use two-factor authentication or multi-factor authentication whenever and wherever. This adds an extra layer of protection and keeps your accounts secure.

Virtual Private Networks (VPNs)
While individuals may have not been aware of this, one can access the internet in a specific region in the world while his/her location is set to another one. This ensures anonymity as it helps users disguise themselves as citizens of other places. The major drawback of this cool tool, :however, is that it can slow down the internet and these VPN services require money. When not using the internet, internet providers can observe each and every thing you do while on the internet. They can even sell your data which could later on be vulnerable for exploitation. VPNs can also protect users from attacks such as man-in-the-middle-attacks by which a malicious third party alters communication between two parties.

Messaging security
Some messaging web and mobile applications such as Signal offer end-to- end encryption services to help keep your communications safe and secure. By using these encrypted platforms, you ensure your data isn’t taken by companies for marketing purposes.

Browser security
Aside from accounts and communication services, browsers can either secure your data or make it vulnerable for all sorts of attacks and exploitations. There are several browsers that offer unique features, but some are better than others. Nonetheless, always make sure to run the latest software.

Software

If you're always up to date with the latest updates, you surely decrease the chances of exploitation and attacks by malicious actors. You should also run the current version of your browser and operating system.

Social engineering

Aside from technological faults, human errors play a major role when it comes to cyber attacks and crimes. Make sure you know how to spot these interaction-based exploitations to keep your computer safe and secure.

Hardening your device

It is the action of making sure your device is as secure as possible from potential attacks. It includes strengthening your OS to enhance protection against cyber attacks. Basically, computers are made up from hardware components and software components. To communicate with this complex machine, operating systems -consisting of software sets- were created to offer computer services and help us individuals interact with computers.

Shared personal security practices

Although each OS differs from one another, all of them share common security practices such as requiring passwords for accounts, limiting administrator access, utilizing firewalls, using trustworthy antivirus software, and offering updates.

Windows Hardening

There are many ways we can use the settings and options of Windows OS to help keep our computers safe. The following checklist can help guide Windows users on securing their devices.

Account Set up:

1) force accounts to have passwords

Open the RUN application on your computer

Type netplwiz

Check the box labeled "Users must enter a username and a password to use this computer"

2) Limit admin privileges
From the user page, select which account you would like to give standard or admin privileges in the group membership page.

3) Require login on screensaver
Open “accounts” in settings
Go to the sign in option
Under the require sign in, select “When PC wakes from sleep”

Security features:
Windows firewall
You can turn it on in the Windows security app in the Firewall and Network protection page

Windows’ built in antivirus software
Go to the windows security app
Go to the setting of the Virus and Threat protection page
Turn on all protection

Disable remote access
Open the control panel
Go to the System and Security page
Go to system and open remote settings
Uncheck the “ allow remote assistance connections to this computer”

Allow automatic Microsoft software updates
Go to update and security in the settings
Go to advanced options
Turn “Receive updates for other microsoft products when you update Windows”

Uninstall unused programs
Not only do they take up space, but also these programs provide extra tools for attackers to employ their malicious activities. Make sure not to accidently uninstall programs for the OS.

Encryption:

If your hard drive doesn’t have built-in encryption, it is time to consider encrypting your hard drive with Bitlocker.

Backup

You can automatically back up using file history and an extra hard drive on some Windows versions

There are also cloud-based back ups such as Onedrive and Dropbox

You can also back up on an external hard drive

Add extra security software

Aside from Windows’ built-in antivirus software which would be sufficient for many individuals, it would always be worth it to invest in an extra layer of protection to enhance the overall security of your PC.

Linux hardening

Linux is an operating system which allows the communication between the software and hardware components of one’s PC. At its most basic, it is a low-level interface known as a kernel which sits between the hardware and the high-level software. Without it, the software wouldn’t work. The linux kernel serves as a building block for Linux versions known as distributions.

To apply any Linux hardening, you have to be familiar with command lines.

Case studies : lessons learned

Organizations should disclose security breaches because not doing so is unethical and illegal.

Don’t store user information in an unencrypted form.

Proper investigations must be done to catch any attack and prevent further damage.

Proper configuration is essential for overall security protection.

Security needs to be proactive and reactive.

Trending topics in cybersecurity (2020s)

New technologies are followed by new security risks.

New emerging technologies provide additional landscapes for hackers to launch their attacks. Thus, the cybersecurity world must be prepared to handle these new types of vulnerabilities by taking effective security precautions.

Cloud computing

It refers to computer services such as servers, databases, software that are hosted over the internet and maintained by the cloud service provider. The cloud offers a space for organizations to grow securely, flexibly, and affordably.

5G

This technology stands for the 5th generation of standards for telecommunications. It is faster and more reliable than its predecessors i.e 4G. This way, communications between devices across the internet become more instantaneous and paves the way for the advancement and evolution of virtual and augmented reality, artificial intelligence, the automation of industries, and even IoT.

Internet of things (IoT)

The internet of things refers to a network of physical devices. The main purpose behind IoT devices is to allow the communication between them and other technologies without user intervention. Examples of IoT include Wi-Fi connected microwaves, thermostats, and self-driving cars. Hence, IoT securing is becoming more and more important as these devices store data which would allow attackers to use them for malicious purposes.

Artificial Intelligence

It is basically the pursuit of making computers intelligent and enabling them to perform complex tasks and make decisions the same way humans can. This evolving field has revolutionized the cybersecurity field as it can be used to assist professionals by analyzing vast amounts of data during a short period of time. Nonetheless, it can also be used for the advantage of attackers