According to Nist , Information security is the protection of information systems from unauthorized access, use, disclosure,disruption, modification, or destruction in order to provide confidentiality, intregrity and availibility.

The CIA Triad

Confidentiality
It's similar to privacy , it s acces to resscources or data must be restricted to only authorized subjects or entities, Data encrption is a comman method for ensuring confid

Integrity
it involves maintaining the consistency and accuracy of data over its entire life cycle, and it's all about making sure information is accurate and always stay that way.

Availability
Ensuring availability requires routine maintenance and upgrading of hardware, software and os to all be up running 24/7

Key Terms

Vulnerability
it s flaw loophole or error that can be exploitated to violate the system security policy

Threat
it's an event, natural or man-made, able to cause negative impact to an organization

Exploit
It's a way to breach the security of an IT system through a vulnerability

Risk
It's a probability of an event that could happen that can expose to danger

Security Threats

Securiy Threats can be **Natural Factors**: Lightning, Hurricane….
It can also be **Human Factor**s divided by **Internal Factors** like Former employers or current employes, **External Threats** like Malicious events like an attack attacking a specefic country Hackers or Cracker**s** or also virus Trjans ad Worms

Vulnerability Assessment

It's the process of identifying analyzing and ranking vulnerabilities in the specefic environment like exploit-db.
They are two points to consider

- Many systems are shipped with known sercurity holes and bugs and insecure default settings
- Misconfiguration by the sysadmin

Type of actors and their motives

There is a lot of actors but the most impotants are :
-Hackers: For example an organization could pay a group of hackers to hack a company and extract their database that is named Operation Aurora
-Internal users: it can be intenational or not the users can be targed by some hackers or he can stick to infect the network
-Hacktivism: Nobody pays hacktivism to perform attacks DDoS campaigns can be made to make pressure for one particular decision, Some Singapore hacktivists performed on the government website they were implementing new compliance and new regulations into their internet.
-Governments: They wants to spy want to understant what is happeing in each country from teh inside from confidential data that they are managing like Russia and Ukrania.

Hacking organizations

-Fancy Bears : DCC hack into Hillary Clinto party
-Anonymous-LaserGroup-Look Sec-Syrian Electronic Army
-Guardian of the peace that hackend Sony in order to get movies

Attack Classification

Passive attacks like traffic analysis
They are hard to detect
Active attacks like DoS, Masquerad(phising), Man in the Middle

Security Services

Service is a processing or communication service that is provided by a system
Sercurity services implements security policies and are implemented by security mechanisms

Security service purpose is enhancing security of data processing systems and information transfers of an organization

Malwares

malicious code or malware is any software used to disrupt computer or mobile operationsto gather inforations…

Types of Mawares:
-Virus it s malware that spreads from one computer to another byt attaching itself to other files using self replication but they require human interaction to self replicate
-Worms it’s a self replicating malware that does not require human interaction

-Troan horses it’s a hiden malware that causes damage to a system or gives an attack access to the host
-Spyware their main goal is to track and report the usage of the host or to collect data that attackers desire to obtain
-Adware it s code that displays or download unsolicited ads usually seen on a browser pop up
-RATs it s stands for remote access tool/trojans. they allow the attacker ro gain unauthaurized access and control the computer
-Rootkit it’s a piece of software that intented to take full or partial control of a system at the lowest level

Ransomeware it’s a malware that infects the host with a code that restricts the access to the computer ot the data on it, the attacker demands ransom to be paid to get back the data if it s not the data will be destroyed

Threat Examples

-Botnet are a set of compromised hosts that enables attackers to exploit thode computer ressources to mount attacks it s used to run DoS, spam, phising, cryptocurrency, the compute part of this are named zombies or drones
-Keyloggers it s any hardware or software that recods every keystroke made by a user
-Logic bombs it s a code that door mounts ona target until it s triggered by a specefic event such as data it can erase date or corrupt the system
-APTs or advanced persistents threats its main goal is to get access and monitor the network to steal information while it’s saying undetected for a long period of a time it s usualy targets organizations such as millitary , government, finace or companies that have hign value infos

Mapping

Before attacking we find our what services are implemented on the network using ping command or using some tools like nmap
Port scanning try to establish TCP connection to each port in sequence 3 handshake

IP Spoofing

IP spoofing is the creation of Internet Protocol (IP) packets which have a modified source address in order to either hide the identity of the sender, to impersonate another computer system, or both.

DoS

it s a flood of maliciously genrated packets “swamp” receiver DDoS means that it s distrbueted to prenvent this we have to filter our flooded packets before reaching the host if we traceback it’s usualy an innocent or compromised machine

Host Insertions

Generally an insider threat , a computer with a malicious intent is inserted in sleeper mode on the network they are quiet it can be a rogue software process inserted onto a host intentionallty we can use it to Network traffic monitoring or also Crypto keys
to prevent this we have to aintain an accurate inventory of computer hosts by MAC address

Cyber Kill Chain

Social Engineering

It s the use of human for cyber purposes

-Phising : impersonnate a website there is a tool like GoPhish or SET
-Vishing: impersonate somebody using the voice like in a call

CIA Triad

Confidentiality: is used to prevent any disclosure without prior authorization byt the owner, for example we can force confid with encryption using a cipher like authentication, access control …

Integrity: it's similar to confidentiality but there is some differences Integrity is the information that we sent or received has not been modified by an unauthorized person of the system
We can implement technical controls such as ciphers or hashes MD5, SHA1
Availability: it s means that data or info is always available when needed we commonly use Backups to always be available
RAIDs : for example if we have 4 hdd and if one is corrupted tothers will be available

Clusters; its the sam as RAIDs but we are dealing with servers
ISP Redundancy for example if a ISP goes down we will have anoher and our internet will be availabe

Non Repudation: it's a valid proof of the identity of the data sender or receiver :
Technical implemetations: Logs & Digital signatures

Access Management

Authorization is the process of allowing somebody to access a specific object .
they are different type of criteria ;
You could be restricted by groups, by time frame or specific dates, also by physical location or transaction type.
All that is SSO stands for Single Sign-on
SSO = user only has to enter their login credentials (username, password, etc.) one time on a single page to access all of their SaaS applications.

Authentication concepts
On the Most systems they will ask you for an identity and authentication for example the username and the paswword will be an identity proof.
The Password willl give authentication and the username will give identification
Kerberos it's a protocol used for implementing cosine on SSO
Mutual auth like CHAP these are some type of authentication processes that aare uses to communicate to systems
SID = In active dir there is something called Security ID it's an ID that identifies a person and it can identify an object like a group or a specific file
DACL = Discretionary Access contreol is a type of access that allows the users to give access to their own data whomever they want

Incident response

Incident management means the information security or the incident managment team will regulary check and monitor the security events occuring on a computer or in our network.
An event is someting that is not part of the normal behaviour of the company , but that is actually an incident so an event could be something that changed the normal behaviour of the system , could be programmed or not is something that change what is the normal process on the company, on the network, on the computer it will be something like access control is update or firewall push it or was updated by someone on the company or logging event in the server
The Incident is the negative part of an event , it s something that will negatively impact the CIA of secreting organization. Normally those incident impact the buisness

So to deal with the incedent we have the response team or commonly known as CCERT is the team that will identify the incident and resolve the issue

For example if somebody goes to the server and disable it this is an event but also an incident so the CCERT team will try to restore the access to the internal network of the company

One important part of the Response team is the investigation, they need to understand what happened , collect evidence in order to understand why this incident happened and who formed it to prevent these incidents from happening again

Key Concepts

E-Discovery: It will allow us to get the current status of all data, all of the systems, all the information that we are dealing with in our computers, in our systems, in our network. Also will allow us to understand how we could control the data retention period and the backups of that data.

Automated Systems: Using SIEMs(Splunk,QRadar,ArcSight) SQA UBA ... , we coulf enhance the mechanism to detect and control incident that could compromise the tech environment

BCP & Disaster Recovery : BCP stands for Buisness Continuity Plan, it's a whole plan that we need to implement in our company in order to prevent ot to guide all the organizations as soon as something happen, Disaster recovery actually is the process that we need to implement or we need to follow in order to be able to recover all the different areas if a disasters occurs

Post-Incident: as soon as everything goes okay , as soon as we recover everything as soon as the services in now up running we will have to investigate why the incident happened what is the root cause

Incident response process

The Cyber Security incident is divided by three different phases :Prepare,Respond,FollowUp

- **Prepare:** You will need to understand if you have the e discovery process. In ohther words , you will need to undestand what kind of systems you are dealing with , do you have administrative controls …
- **Repond:** You will need to identify what is the CyberSecurity Incident for example if somebody cam here into your office and leave an plug it into your computer and our became infected. The way Dealing with cyber security incident is different than the way dealing with security incident or another kind of incident. Then after we will have to trigger the Buisness Continuity Plan if the incident required it.
- **Follow up:** You will need to investigate like why it happened ….

Firewalls

It's a protection mechanisms that isolates organization's internal net from larger Internet, Allowing some packets to pass, blocking others. Firewalls generally used to separate the internal entreprite that has the application of security policies from publiv internet where WWW stands for Wild Wild West that just no a shred of security applied to that.

- **Prevent DoS:** Syn flooding: attacker establishes many bogus TCP connections, no ressources left for "real" connections
- **Prevent llegal modification/access of internal data :** e.g attackers replaces CIA's homepage with something else
- **Allow only authorized access to inside network**
- **Two types of firewalls:** Application level and packet filtering

Firewall - Packet Filtering

Router filters packet -by-packet, decision to forward/drop packet based on :

- source IP , destination IP
- TCP/UDP source and destination port numbers
- ICMP message type
- TCP , Syn and ACK bits

Firewall - Application Gateway

Filters packets on application data as well as on IP/TCP/UDP fields

Firewall - XML Gateway

XML is a transport protocol that moves document, communication … it uses port 80 on a firewall and port 80 is standard web traffic port, it's left open

Types of Firewalls

- **Stateless Firewalls :** They have no concept of the state it can also be called packet filters, They make their decisions based on layer three and layer four information meaning IP and Port. They lacked sense of the state , and of course they are less secure
- **Stateful Firewalls :** It basically allowed the firewall to compare current packets with previous packets. This actually makes the firewall a little bit slower, but fare more secure than their stateless firewall , sometimes it's also called Application Firewalls, and they can make decisions based on layer 7 infomation meaning they could also filter informations based on the type of website that somebody is listening
- **Proxy Firewalls :** They act as an intermediary server it's like MITM they are 3 handshakes

Antivirus/Antimalware

- **An antivirus** is a specialized software that can detect, prevent and even destroy computer viruses or malware. This specialized software use model with definitions. They are basically like signatures for identifying malicious software or malware.
- **Most antivirus** software works by comparing each file encountered on your system against a compressed version of known malware maintained by the vendor on the local host

For example we get one files infected, you will actually match hash for example a md5 hash that is already recognizes malware
The most common one we ll be a host based antivirus system that is actually connected to a centralized server

Cryptography

Cryptography it's basically a way of secret writing. it's a secure communication between two parties, and only the intended recepient can understand this communication .
Cryptography isn't new it was used for thowsand of years for example egyptian hieroglyphics, Caesar Cipher …

Cryptography - Key Concepts

- **Confidentiality** is the process of assuring that only the intended parties can read and understand the message
- **Integrity** is the process of actually detecting if the message has been changed where the messages shouldn't be altered in any way in the process of beinf transmitted
- **Authentication** it's process of identifying are authenticated with someone or something or some message is actually correct
- **Non-repudiation** is the process of detecting if something or someone has done something
- **Cryptanalysis** is basically the process of analyzing ciphers in cryptographic algorithms
- **Cipher** is the actual algorithm that encrypts a message
- **Plaintext** is human readable
- **Ciphertext** basically refers to the plaintext gone trough the cipher , which is has been applied to a plaintext and the ciphertext is something that it's not humanly readable
- **Encryption** is the process of transforming plaintext into ciphertext
- **Decryption** is the process of transforming ciphertext into plaintext using the cipher

Cryptography - Strength

Cryptography strength relies on math not secrecy keeping something secret does not make a cryptographic algorithm anymore secure.

Stream cipher & Block cipher

- Stream cipher encrypt or decrypt information bit per bit
- Block cipher they encrypt or decrypt information differently. They are actually use blocks of bits or bites to encrypt informations

Types of Cryptography

There are three types of modern encryption:

- **Symmetric Encryption:** it uses the same key to encrypt and decrypt and its security depends on keeping it secure all the time and the bigger key the stronger the algorithm
- **Asymmetric Encryption:** We have 2 keys one key can be made publicly called public key and the other one needs to be kept private at all times it s called private key, since we have 2 keys one key is used to encrypt and the other to decrypt. And it's actually smaller than symmetric encryption and this is a reason why whenever we use asymlectruc encryption most of the time we are using symmetric encryption as well
- **Hash Functions :** it's provide one way encryption algorithm and no key. This means that any lenght or variable lenght plaintext is hashed into a fixed lenght hash value

A collision means two different plaintext having the same hash

Cryptographic attacks

- **Brute force** is an attack based on trial and error and effectivelly would work trought submission of many passwords or fast traces to hope that eventually it will guess correctly
- **Rainbow tables** are similare but they are limited amount of information or entity or files
- **Social engineering** consits using non-technical methods to get those maybe get the password from the end users themselves
- **The Known Plaintext** it's an attack based on having only plaintext and doing analysis based on that plaintext to try to understand how the cipher works
- **The Known Ciphertext** is an attack based on having only ciphertext and we try to defer the key used in the cipher to again encrypt information