The CIA Triad

The CIA Triad is a fundamental principle in cybersecurity that serves as a guiding framework for protecting information and systems. It consists of three core elements: Confidentiality, Integrity, and Availability.

Confidentiality

Confidentiality refers to the protection of sensitive information from unauthorized access or disclosure. It ensures that data is only accessible to authorized individuals or entities.

So, while dealing or testing for the confidentiality, we have to ask us a simple question.

Can actors who should not have access to the system or information can still access it?

If the answer is Yes. Then, we have to implement some measures like Encryption techniques, Access Controls that include passwords and biometrics and data classification and labelling.

Integrity

Integrity involves maintaining the accuracy, completeness, and trustworthiness of data throughout its lifecycle. It ensures that information is not modified or tampered with by unauthorized parties, whether intentionally or accidentally.

The question we have to ask here is

Can the data or the system be modified in some way that is not intended?

If the answer is Yes. Then, we have to implement some digital signatures and hashing, Version control and auditing and input validation and sanitization.

Availability

Availability ensures that authorized users have reliable and timely access to information and resources when needed. It focuses on ensuring the continuity of operations and preventing disruptions or denial of service.

Here, the question we have to ask is

Are the data or the system accessible when and how they are intended to be?

If the answer is No, then we have to implement some Redundancy and failover systems, Load balancing and scalability and a Disaster Recovery plan.

Summing it all up. We can see the CIA Triad as three 3 pillars of information security. If a data, lets say your gmail account can be accessed by anyone over the internet and then he/she can read all your emails or messages. without any password Then, we are lacking the Confidentiality implementation there.

For the integrity, let say you send a message to your colleague stating that you love their work but a hacker sitting in between you and your colleague changes the message from i love your work to i hate your work. Then, it will comes under the integrity issue where you cannot confirm the authenticity of the message or the data. Combining, it with confidentiality can cause even bigger bundle.

Let say, a hacker hack into a hospital and accessed their medical records. At this point, he had already destroyed the confidentiality pillar but instead of only looking into the records of the patient, he also made changes in them. Now, this will come under both confidentiality and integrity issue.

At last, we had the availability. Those of you who are from India, can relate to it very easily. Whenever there is a result declaration of any 10th or 12th boards exam. The government website that day takes even more time to load than it normally does. Because on that day, there is a high number of traffic on the website which the server infrastructure cannot hold. So, it kinda crash out, destroying the availability pillar of our CIA Triad.
