

## ***Lecture 1 – 27/02***

### ***Cybersecurity***

is the practice of protecting digital systems, networks, and data from unauthorized access, alteration, or destruction. It encompasses various technologies, processes, and practices designed to safeguard information assets against a wide range of cyber threats.

### ***Data***

è il cuore delle aziende e organizzazioni e include gestione dell'inventario, vantaggi competitivi, incremento della quota di mercato, miglioramento di prodotti/servizi.

### ***Data loss/damage:***

- **Financial loss:** Regulatory bodies impose strict requirements for data protection and privacy. Failure to comply with these regulations can lead to fines, lawsuits, and other legal consequences.
- **Reputation damage:** entities/organizations failing to protect data, risk damaging their reputation and losing the trust of customers, partners, and stakeholders
- **Legal ramifications:** Regulatory bodies impose strict requirements for data protection and privacy. Failure to comply with these regulations can lead to fines, lawsuits, and other legal consequences.

Gli ***obiettivi del DNS*** sono:

- **Confidentiality:** Proteggere le informazioni sensibili da divulgazioni non autorizzate tramite crittografia, controlli di accesso e politiche di classificazione dei dati.
- **Integrity:** Garantire accuratezza e affidabilità dei dati prevenendo modifiche non autorizzate con validazione dei dati, checksum, firme digitali e controlli di accesso.
- **Availability:** Assicurare che dati e risorse siano accessibili agli utenti autorizzati quando necessario, implementando ridondanza, tolleranza ai guasti, piani di recupero e protezione da attacchi DoS.

### ***Malware***

A type of software program or code specifically designed to infiltrate, damage, disrupt, or gain unauthorized access to computer systems, networks, or devices, often with malicious intent.

### ***Covert Channel***

È un canale di comunicazione indiretto tra parti non autorizzate che viola una politica di sicurezza, sfruttando risorse condivise in modo non previsto per aggirare i meccanismi di controllo.

### ***Advanced Persistent Threats (APT)***

Sono attacchi informatici sofisticati e mirati in cui un'entità non autorizzata ottiene accesso a una rete e rimane inosservata per un lungo periodo.

### ***Proprietà sensibili di un dataset***

- **informazioni demografiche:** età, genere, etnia, livello di reddito.
- **modelli comportamentali:** abitudini di acquisto, cronologia di navigazione, interazioni sociali.
- **preferenze personali:** affiliazioni politiche, condizioni di salute, scelte di stile di vita.

La loro divulgazione può portare a violazioni della privacy, discriminazione o manipolazione.

I **livelli del web** sono:

- **Surface Web**
- **Deep Web**
- **Dark Web**

### ***Digital Forensics***

Branch of forensic science that deals with the identification, preservation, examination, analysis, and presentation of digital evidence derived from electronic devices and digital media. Its goal is to explain current state of a digital artifact.

### ***GDPR***

È una legge europea entrata in vigore il 25 maggio 2018. Stabilisce norme per la protezione dei diritti fondamentali e delle libertà delle persone, in particolare il diritto alla protezione dei dati personali. Ha lo scopo di migliorare la protezione dei consumatori e il livello generale di privacy, prevede la segnalazione obbligatoria delle violazioni dei dati e pone maggiore enfasi sul consenso esplicito per il trattamento delle informazioni.

Nel **Networking Tradizionale**, i piani di controllo (che determinano l'inoltro dei pacchetti) e dati (che gestisce l'inoltro effettivo dei pacchetti) sono strettamente integrati nei dispositivi di rete.

### ***Software Defined Networking (SDN)***

This separation allows for programmability and automation of network configurations and policies. This enables network administrators to dynamically control and manage network traffic flows according to application requirements and business needs.

### ***Social Bots - Spam Bots***

Sono account (semi-)automatizzati progettati per imitare il comportamento umano sulle piattaforme social, con intenti dannosi come la diffusione di disinformazione, il furto di dati personali, la manipolazione del mercato azionario e l'influenza politica.

### ***Authentication***

È il processo di verifica dell'identità di un utente, con gli obiettivi di stabilire fiducia, prevenire accessi non autorizzati e proteggere informazioni sensibili.

### ***Cyber Deception***

È una strategia di cybersecurity che mira a ingannare e manipolare gli aggressori che tentano di violare una rete o un sistema. Consiste nella creazione deliberata di informazioni false, esche, trappole ed elementi ingannevoli per deviare, confondere o ritardare gli attaccanti, migliorando così la sicurezza dell'organizzazione.