Seminario 6

Questo seminario parla di direttive nazionali ed europee per la salvaguardia della sicurezza informatica e per l'aumento della resilienza delle infrastrutture.

Strategia Europea di Cybersecurity

La **Strategia Europea per il Decennio Digitale** (16 dicembre 2020) mira a garantire un Internet globale e aperto, tutelando al contempo la sicurezza e i diritti fondamentali delle persone in Europa. Gli strumenti principali per questa strategia sono:

1. **Regolatori**: Normative che stabiliscono obblighi minimi di sicurezza.
2. **Investimenti**: Fondi per potenziare le infrastrutture e le competenze.
3. **Policy**: Linee guida per coordinare azioni strategiche nei settori della resilienza tecnologica, capacità operativa e cyberspazio globale e aperto.
   Questa strategia favorisce la collaborazione tra Stati membri per rafforzare la resilienza delle infrastrutture critiche, la giustizia, la diplomazia informatica e la ciberdifesa.

Strategia Nazionale di Cybersicurezza (2022/26)

L’obiettivo della **Strategia Nazionale** è affrontare sfide legate alla transizione digitale, promuovendo un uso sicuro delle tecnologie per:

- Rafforzare la resilienza e anticipare le minacce cyber.
- Gestire crisi cibernetiche in contesti geopolitici complessi.
- Contrastare la disinformazione online, rispettando diritti umani e valori nazionali.
  Un ruolo chiave è svolto dal **Piano Nazionale di Ripresa e Resilienza (PNRR)**, che include investimenti nella digitalizzazione della Pubblica Amministrazione e progetti come il Cloud Nazionale.

CVCN - Centro di Valutazione e Certificazione Nazionale

Il potenziamento del **CVCN** dell'agenzia per la Cybersicurezza Nazionale e dei Centri di Valutazione (**CV**) del Ministero dell'interno e della Difesa è centrale per garantire la sicurezza delle infrastrutture ICT nazionali. Le sue azioni includono:

• Sviluppo di linee guida per la Pubblica Amministrazione basate sull'approccio **Zero Trust**.
• Creazione di una politica nazionale per la divulgazione coordinata delle vulnerabilità.
• Potenziamento della rete di laboratori accreditati per valutare e certificare le tecnologie critiche.

> **Info**
>
> Il modello **Zero-Trust** si fonda sul principio della verifica continua e della minima fiducia. Presuppone che nessuna entità, sia essa interna o esterna alla rete aziendale, sia intrinsecamente affidabile.

NIS 2

La **NIS 2** (Network and Information Security 2) è una direttiva dell'Unione Europea introdotta per migliorare la sicurezza informatica delle infrastrutture critiche e dei servizi essenziali in Europa. Nasce come evoluzione della precedente direttiva NIS, per affrontare le lacune emerse e rispondere al crescente numero di attacchi informatici.

Essa stabilisce standard minimi di sicurezza, obblighi più rigorosi per le organizzazioni critiche e un quadro di cooperazione più solido tra Stati membri. Copre un ambito più ampio di settori, tra cui energia, trasporti, sanità e servizi digitali avanzati, con l'obiettivo di aumentare la resilienza delle infrastrutture e la capacità di risposta agli incidenti cyber.

Si integra con la legge italiana sul **Perimetro di Sicurezza Nazionale Cibernetica**, fornendo un quadro completo per la protezione delle infrastrutture critiche.

Cybersecurity Act

Il **Cybersecurity Act**, introdotto nel 2019, è un pilastro fondamentale per rafforzare la sicurezza informatica nell'UE. Esso mira a creare un **quadro di certificazione comune** per i prodotti, i processi e i servizi digitali, aumentando la fiducia degli utenti e la coerenza delle normative.

Le principali caratteristiche del Cybersecurity Act sono:

- **Certificazione Europea**: Viene istituito un sistema unico di certificazione della sicurezza informatica valido in tutta l'UE, che sostituisce gli schemi nazionali. Ciò garantisce che prodotti e servizi certificati siano riconosciuti in ogni Stato membro.

- **Ruolo rafforzato dell’ENISA**: L’Agenzia dell’Unione Europea per la Cybersecurity assume un ruolo centrale nel supportare gli Stati membri e nel coordinare le attività di certificazione.
- **Standard di sicurezza uniformi**: I prodotti certificati devono rispettare requisiti uniformi di sicurezza, garantendo protezione contro le minacce informatiche su scala europea.