StatCities 2025
GO Stats! Le misure dei territori
Gorizia, 8 e 9 maggio 2025

Cybersicurezza e IA: integrità e sicurezza delle banche dati.

Giuseppe Sindoni - Istat

Comune
di Gorizia

Unione Statistica Comuni Italiani

Perché l'enfasi sulla cybersicurezza?

- **A livello globale il primo semestre del 2024 è stato il peggiore di sempre, con 1.637 eventi malevoli di una certa rilevanza, con +23% rispetto al 2023 (Rapporto Clusit 2024)**
- **Dal 2019 in Italia sono stati rilevati 777 incidenti noti di particolare gravità, con un lieve calo nel primo semestre del 2024 rispetto al 2023**
- **Crescenti tensioni geopolitiche che contribuiscono a scenari sempre più incerti (WEF Global Cybersecurity Outlook)**
- **Crescenti complessità delle catene di approvvigionamento per le organizzazioni, che diminuiscono il grado di predicibilità dei rischi**
- **Nuove vulnerabilità portate dalle tecnologie emergenti**
- **Crescita (ipertrofica?) del corpus normativo che impone nuovi adempimenti alle organizzazioni**

Questa foto di Autore sconosciuto è concesso in licenza da CC BY-SA-NC

Cybersicurezza…

- … o sicurezza informatica?
- Secondo la direttiva NIS2 della UE, cybersicurezza e sicurezza informatica sono sinonimi:

La sicurezza informatica comporta la protezione delle reti e dei sistemi informativi (NIS), dei loro utenti e di altre persone interessate da incidenti e minacce informatiche.

Sicurezza informatica non coincide con sicurezza delle informazioni.

La prima si rivolge agli oggetti informatici (impianti, reti, dispositivi, sistemi, applicazioni, servizi),

la seconda mira a mettere in sicurezza il bene "informazione" nelle dimensioni:

organizzazione, fisica ed ambientale, logica (cioè tecnologia informatica o telematica).

- Per la sicurezza delle informazioni la sicurezza informatica è una parte ed è un mezzo, non è la finalità. (Wikipedia)

Recenti sviluppi normativi

- La direttiva NIS 2 della UE mira a rafforzare la sicurezza informatica in Europa, estendendo gli obblighi di sicurezza e reporting a un numero maggiore di settori critici, come energia, trasporti e salute. Introduce requisiti più rigorosi per la gestione dei rischi e la cooperazione tra gli Stati membri per affrontare le minacce informatiche.
- La legge 138 del 2024, tra le altre cose:
  - Recepisce la NIS 2
  - Obbliga i soggetti a cui si applica la legge a istituire una struttura per la cybersicurezza, che riferisce al vertice e si interfaccia con l'ACN (tra i soggetti ci sono le città metropolitane, i comuni con popolazione superiore a 100.000 abitanti e i comuni capoluoghi di regione)

Che c'entra la IA con la cybersicurezza?

La sicurezza di un sistema di IA può essere definita come l'insieme di strumenti, strategie e processi implementati per identificare e prevenire le minacce e gli attacchi che potrebbero compromettere la riservatezza, l'integrità o la disponibilità di un modello di IA o di un sistema abilitato all'IA.

Come tassonomia di riferimento per gli attacchi ai sistemi di IA può essere usata quella sviluppata dal NIST che prevede le seguenti macro-categorie di attacchi:

- **Evasion attacks**: categoria di attacchi che ha come obiettivo quello di generare un errore nella classificazione del modello introducendo perturbazioni negli input del modello, denominate «adversarial examples»;
- **Poisoning attacks**: categoria di attacchi che ha come obiettivo quello di degradare le prestazioni di un modello o fargli generare uno specifico risultato alterando i dati di addestramento del modello;
- **Privacy attacks**: categoria di attacchi che ha come obiettivo quello di compromettere le informazioni degli utenti ricostruendole a partire dai dati di addestramento;
- **Abuse attacks**: categoria di attacchi che ha come obiettivo quello di alterare il comportamento di un sistema di IA generativa per adattarlo ai propri scopi come, ad esempio, perpetrare frodi, distribuire malware e manipolare informazioni.

Nota: Alla luce di questo, la PA deve adottare un'efficace processo di gestione dei rischi per l'adozione dell'IA. Un framework efficace riportato nelle Linee Guida è rappresentato dal Risk Management Framework per l'IA (AI RMF) del NIST che è composto da 4 funzioni: GOVERN (definire la gestione del rischio); MAP (identificare il rischio) ; MEASURE (monitorare il rischio); MANAGE (agire sul rischio).

Ma noi concretamente cosa possiamo fare?

Grazie!

sindoni@istat.it