Infrastrutture Critiche e Sicurezza Nazionale: la Roadmap CISA per l'Intelligenza Artificiale 2023-2024

La "Roadmap for Artificial Intelligence 2023-2024" della Cybersecurity and Infrastructure Security Agency (CISA), un'agenzia del Dipartimento della Sicurezza Interna degli Stati Uniti (DHS), rappresenta un piano strategico cruciale che risponde direttamente all'Ordine Esecutivo 14110 della Casa Bianca. Questo documento è fondamentale per garantire lo sviluppo e l'uso sicuri e affidabili dell'intelligenza artificiale (AI), allineandosi strettamente con le direttive nazionali degli Stati Uniti. L'obiettivo centrale della roadmap è quello di massimizzare i benefici dell'AI per potenziare la cybersecurity e proteggere le infrastrutture critiche, assicurando al contempo la sicurezza dei sistemi AI da eventuali minacce informatiche e contrastando l'uso inappropriato dell'AI che potrebbe mettere in pericolo le infrastrutture critiche.

La roadmap si sviluppa attraverso cinque punti principali, ognuno dei quali sottolinea un aspetto specifico dell'integrazione dell'AI nei contesti legati alla sicurezza nazionale:

1. **Utilizzo Responsabile dell'AI**: CISA si impegna a utilizzare l'AI in modo etico e sicuro, nel rispetto delle leggi e delle politiche, per rafforzare la difesa cibernetica e supportare la sua missione di protezione delle infrastrutture critiche.

2. **Valutazione e Assicurazione dei Sistemi AI**: la roadmap include la valutazione e l'assistenza per l'adozione di software AI "secure by design" da parte di una vasta gamma di stakeholder. Questo sforzo mira a stabilire pratiche e linee guida per lo sviluppo e l'implementazione resiliente dell'AI.
3. **Protezione delle Infrastrutture Critiche**: uno sforzo chiave è la valutazione e la raccomandazione di strategie per mitigare le minacce AI alle infrastrutture critiche, in collaborazione con altre agenzie governative e partner industriali.
4. **Collaborazione e Comunicazione**: CISA lavora con partner internazionali e inter-agenzia per sviluppare politiche e strategie comuni per la sicurezza AI, promuovendo la cooperazione e la condivisione delle migliori pratiche a livello globale.
5. **Educare la Forza Lavoro**: L'agenzia si impegna a formare la propria forza lavoro sugli aspetti tecnici, legali, etici e politici dei sistemi software AI, continuando contemporaneamente a reclutare personale specializzato in AI.

In sintesi, la Roadmap di CISA per l'AI si concentra sull'integrazione di principi "Secure by Design" nei sistemi AI, enfatizzando la necessità di sicurezza come requisito fondamentale e integrato nello sviluppo dei sistemi AI fin dall'inizio e per tutto il loro ciclo di vita. La collaborazione tra governo, industria e accademia è essenziale per stabilire le linee guida necessarie per garantire che gli strumenti software basati su AI siano sicuri e affidabili.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/infrastrutture-critiche-e-sicurezza-nazionale-la-roadmap-cisa-per-lintelligenza-artificiale-2023-2024/