Intelligenza artificiale e sicurezza, quali nuove minacce informatiche? Il report ENISA

Dopo la pubblicazione del report delle nuove minacce informatiche nelle reti quinta generazione, l'agenzia dell'**Unione europea per la sicurezza informatica** ha pubblicato il rapporto sul panorama delle minacce cyber anche nel settore dell'intelligenza artificiale, svelando le principali sfide alla sicurezza informatica che l'ecosistema dell'IA deve affrontare.

Nel report **"AI Threat Landscape" l'ENISA** sottolinea l'importanza della sicurezza informatica e della protezione dei dati in ogni parte dell'ecosistema AI per creare una tecnologia affidabile per gli utenti.

Lo studio dell'agenzia per la sicurezza adotta un approccio metodologico per mappare i principali attori e minacce nell'IA. La relazione fa seguito alle priorità definite nel Libro bianco sull'IA 2020 della Commissione europea.

Intelligenza artificiale e cybersecurity

Il nuovo lavoro dell'agenzia mira a fungere da base per le iniziative per proteggere l'IA: sia in termini di politiche, poiché inquadra il problema e fornisce indicazioni sulle minacce alla sicurezza informatica, sia in termini di controlli tecnici, in quanto evidenzia minacce specifiche per

quale azione può essere necessaria.

Il rapporto è diretto ai responsabili delle politiche quando sviluppano linee guida future sulle implementazioni sicure dell'IA, agli esperti tecnici per supportare valutazioni del rischio personalizzate e agli organismi di standardizzazione per supportare i futuri standard di sicurezza dell'IA.

Il panorama delle minacce dell'IA dell'ENISA identifica le sfide e le opportunità per implementare sistemi e servizi di IA sicuri in tutta l'Unione. Il rapporto sottolinea la necessità di misure di sicurezza più mirate e proporzionate per mitigare le minacce individuate, nonché la necessità di un'analisi approfondita dell'uso dell'IA in settori come la salute, l'automotive e la finanza.

Per approfondire

https://www.key4biz.it/intelligenza-artificiale-e-sicurezza-quali-nuove-minacce-informatiche-il-report-enisa/335531/