PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 28 - numero 6204 di Venerdì 27 novembre 2026

Un manuale per rafforzare le difese e gestire i rischi degli attacchi informatici

Il manuale GAO analizza il ruolo dell'intelligenza artificiale nella cybersicurezza, illustrando come può essere utilizzata per individuare le minacce, rafforzare le difese e affrontare i rischi legati alla sua applicazione negli attacchi informatici.

È noto come gli applicativi di intelligenza artificiale possono potenziare l'impatto di attacchi informatici. Parimenti, un appropriato uso di questi applicativi può contribuire in modo determinante a contrastare questi attacchi.

Ricordiamo ai lettori che un applicativo "***agentic AI***" è un sistema AI che opera con un livello di autonomia elevatissimo, potendo assumere in modo indipendente decisioni e comportamenti adattivi. Questo tipo di applicativo può essere usato sia per potenziare gli attacchi informatici, sia per migliorare le difese informatiche.

Ad esempio, un appropriato applicativo può analizzare il traffico in rete e mettere in evidenza situazioni anomale. Parimenti, applicativi intelligenti possono effettuare una scansione dei sistemi, mettendo in evidenza possibili debolezze.

Pubblicità

Tuttavia, questi applicativi devono fronteggiare delle sfide non indifferenti, in quanto ancora oggi gli esperti non hanno stabilito delle regole uniformi per valutare se un determinato applicativo abbia capacità offensive o difensive.

Ad esempio, gli esperti hanno già identificato queste aree di rischio:

- sfide afferenti alla protezione dei dati ed alla qualità dei dati,
- sfide tecniche che riguardano la architettura degli applicativi AI generativi,
- ostacoli dovuti all rapido sviluppo di questi applicativi ed a sistemi informatici non sufficientemente aggiornati,
- ostacoli organizzativi, come ad esempio il costo di questi applicativi.

Nel volume allegato a questa nota vengono identificati quattro obiettivi primari, afferenti all'uso di AI nell'ambito della sicurezza informatica.

Ecco i quattro obiettivi identificati ed ampiamente illustrati:

- individuare per tempo aree di debolezza nei sistemi informatici,
- approfondire le ricerche afferenti a questi applicativi,
- tenere sotto controllo questi applicativi per tutto il loro ciclo di vita,
- potenziare le risorse umane messi a disposizione della sicurezza informatica.

Chi scrive raccomanda caldamente ai responsabili della sicurezza informatica aziendale di leggere attentamente il documento allegato, che rappresenta, almeno ad oggi, lo stato dell'arte nell'ambito degli attacchi e delle difese, afferenti a sistemi ***agentic AI***.

GAO ? NOVEMBER 2026 - TECHNOLOGY ASSESSMENT - AI and Cybersecurity - Technologies Can Magnify Cyberattacks and Enhance Cyber Defense - intelligenza artificiale e cybersicurezza - Le tecnologie possono amplificare gli attacchi informatici e rafforzare la difesa.

Adalberto Biasiotti

Licenza Creative Commons
I contenuti presenti sul sito PuntoSicuro non possono essere utilizzati al fine di addestrare sistemi di intelligenza artificiale.

---

www.puntosicuro.it