OUCH! 2023. május

Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

Amit érdemes tudni a mesterséges intelligenciáról

Mi ez és miért érdemes odafigyelnünk rá?

A mesterséges intelligencia (MI vagy AI, az angol Artificial Intelligence-ből) olyan rendszereket jelent, amelyek úgy vannak programozva, hogy emberként gondolkodjanak és reagáljanak. Valójában ezt a meghatározást is egy mesterséges intelligencia rendszer, a ChatGPT adta a kérdésünkre.

Mi az a mesterséges intelligencia?

Az MI az emberi intelligencia szimulációját jelenti olyan gépekben, amelyek úgy vannak programozva, hogy emberként gondolkodjanak és tanuljanak. Olyan algoritmusok és programok fejlesztését foglalja magában, amelyek képesek a jellemzően emberi értelmet igénylő feladatok elvégzésére, mint például a beszéd felismerése, a természetes nyelv megértése, a döntéshozatal és a játék. A mesterséges intelligenciának többféle típusa létezik, ideértve a szabályalapú MI-t, a szakértői rendszereket és a gépi tanulást.

Az MI erőssége abban rejlik, hogy képes szimulálni az emberi intelligenciát és gondolkodási képességet, azonban bármely embernél nagyságrendekkel több információt képes elemezni, sokkal rövidebb idő alatt.

Az MI koncepciója nem új keletű. Az elsőként a sci-fi irodalomban feltűnt MI-t, már évtizedek óta kutatják és fejlesztik. Manapság azért hallunk róla annyit, mert ez az első alkalom, hogy bárkinek lehetősége van kapcsolatba lépni egy MI-vel és megtapasztalni a képességeit.

Az egyik első nyilvánosan elérhető megoldás a ChatGPT, ami egy olyan online mesterséges intelligencia csevegőbot, amely képes úgy reagálni, mint egy igazi ember, és a Turing-teszten is átment. Ezzel a teszttel megállapítható, hogy egy gép intelligens viselkedést tanúsít-e, miközben egy valódi emberrel lép interakcióba egy szöveges felhasználói felületen keresztül. Ha a teszten résztvevő személy nem tudja megállapítani, hogy géppel vagy emberrel kommunikál-e, akkor a gép átment a teszten. A ma elérhető MI rendszerek az első olyanok, amelyek erre képesek.

Az online beszélgetés azonban csak a kezdete annak, amire a mesterséges intelligencia képes. Manapság már léteznek MI megoldások, amelyekkel például oktatóvideó készíthető bármely nyelvhez; az egészségügyi adatok elemzésével meghatározható, hogy kinél a legvalószínűbb a rákos megbetegedés kialakulása; híreket vagy esszéket írnak tetszőleges témában; képeket készíthetnek gyermekkönyvekhez vagy akár új számítógépes programokat is képesek írni. Noha a mesterséges intelligencia nem feltétlenül olyan dolog, amitől tartani kell, vannak veszélyek, amelyekkel érdemes tisztában lennünk.

A mesterséges intelligencia veszélyei

1. **Leutánozhat bennünket**: Az MI-megoldások képesek rögzíteni a hangunkat, majd valós időben létrehozni olyan új hangot, amely pontosan úgy szól, mint az eredeti, ezzel megszemélyesítve minket. Egy kibertámadó ily módon létrehozhat mesterséges telefonos hangüzeneteket, és elhitetheti munkatársainkkal, bankunkkal vagy egy családtagunkkal, hogy mi telefonálunk és bármire megkérheti őket a nevünkben. Az MI ugyanezt képekkel vagy videóval is megteheti. Egy mesterséges intelligencia-megoldás, amelyet Deep Fake-nek hívnak, egy meglévő képet vagy videót felhasználva teljesen új képeket vagy videókat hozhat létre rólunk (beleértve a hangunkat is), amelyen olyan események történnek, amiket soha nem csináltunk.

2. **Rossz válaszok**: Az MI által biztosított adatok és válaszok hibákat, tévedéseket tartalmazhatnak. A mesterséges intelligencia gyakran használ az Interneten keresztül elérhető nyilvános információkat, illetve válaszait a fejlesztők elfogultsága is befolyásolhatja. Míg a tipikus keresőmotorokat úgy tervezték, hogy a „legjobb" vagy leghelyesebb választ adják a kérdéseinkre, az olyan megoldások, mint az MI a leginkább emberszerű választ próbálják adni. Hogy melyik a jobb, az attól függ, hogy mit szeretnénk elérni.

3. **Nem mindenki egyenlő**: Mivel a mesterséges intelligencia a legújabb, legmodernebb technológiának számít, cégek százai kínálnak különböző MI-szolgáltatásokat. Sokan közülük az adatainkat vagy hitelkártyánk adatait szeretnék felhasználni. Legyünk óvatosak! – Nem minden MI-szolgáltatás megbízható. Tájékozódjunk, mielőtt regisztrálunk vagy használatba veszünk egy mesterséges intelligencia-szolgáltatást!

4. **Adataink védelme:** Amikor mesterséges intelligencia rendszert használunk vagy interakcióba lépünk vele – például online csevegünk a ChatGPT-vel – legyünk tudatában annak, hogy a rendszerbe bevitt információk nemcsak feldolgozásra, hanem megőrzésre is kerülnek, sőt a mások számára adott válaszokban felhasználásra is kerülhetnek. Ez azt jelenti, hogy ha bármilyen személyes adatot vagy bizalmas munkahelyi információt is megadunk, ezek az információk tárolásra, így potenciálisan megosztásra vagy eladásra is kerülhetnek. Ne osszunk és ne adjunk meg semmilyen olyan információt, amelyet érzékenynek, személyesnek tartunk vagy bizalmas munkahelyi információt tartalmaz!

Az MI jövője

A mesterséges intelligencia még mindig gyerekcipőben jár, hasonlóan ahhoz, ahol az Internet volt húsz-harminc évvel ezelőtt. Bár számíthatunk a mesterséges intelligencia gyors fejlődésére és alkalmazására, nagyon nehéz megjósolni, hogy milyen lesz a hatása. Legyünk tudatában annak, hogy ezek a képességek rendelkezésre állnak, és mesterséges intelligencia használatakor legyünk nagyon óvatosak azzal kapcsolatban, hogy milyen információkat adunk és osztunk meg!

Források

ChatGPT: https://chat.openai.com/chat
Turing Test: https://en.wikipedia.org/wiki/Turing_test

A fordítást készítette: Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI)