Biztonsági kihívások a mesterséges intelligencia alapú projektekben

2024 január 17.
Ernst & Young Consulting Ltd.

The better the question. The better the answer.
The better the world works.

Building a better working world

AGENDA

I. Adatvédelmi kihívások az MI Projektjeiben

II. Hibrid fenyegetések az MI használatával

III. Tanuló modellhez kapcsolódó visszaélések

IV. Biztonsági védekezés lehetőségei

Adatvédelmi kihívások az MI Projektjeiben

Milyen kihívásokkal szembesülünk az MI alapú projektekben?

1. MI adatokhoz való hozzáférés és adatkezelés?
2. Adatminőség és megbízhatóság?
3. Adatok anonimitása és személyes adatok védelme?
4. Adatok tulajdonjoga és a szükséges engedélyek?
5. Adatvédelmi szabályozások betartása?
6. Adatbiztonsági incidensek és azok kezelése?
7. Etikai megfontolások és társadalmi elfogadottság?

Hibrid fenyegetések az MI használatával

Megjelennek-e új típusú fenyegetettségek az MI elterjedésével?

Az MI és a hagyományos kibertámadások együttes használata új típusú támadási formákat, intenzitást és sikerességi arányt biztosít.

Hogyan használják az MI-t a kiberbűnözők a támadásaik során?

1. Adathalászat és támadások személyre szabása
2. Rosszindulatú szoftverek/exploitok fejlesztése
3. Támadási forgatókönyvek és automatizálás
4. Sérülékenységek feltérképezése

Tanuló modellhez kapcsolódó visszaélések

Lehet-e befolyásolni az MI által visszaadott eredményt?

Az MI által visszaadott eredményeket alapjaiban határozza meg az a tanuló modell, amit a betanításhoz felhasználtak, illetve a további tanításhoz használnak.

Milyen manipulációk érhetik a tanuló modelleket?

1. Adathamisítás
2. Adversarial Attacks
3. Privacy Attacks (Adatvédelmi támadások)

Biztonsági védekezés lehetőségei

Hogyan védekezhetünk az új típusú támadások ellen?

MI specifikus IT biztonsági területek:

1. MI-hez köthető támadások összesítése, kutatása
2. Adatvédelem
3. Modellek validálása

Klasszikus IT biztonsági követelmények MI specifikus megoldásai:

1. Monitoring
2. Hálózatbiztonság
3. Szakemberek speciális képzése
4. Biztonsági mentés és visszaállítás
5. Hozzáférés ellenőrzés

Köszönjük a figyelmet!

Minden harmadik válaszadó (36%) arra számít, hogy **olyan sikeres támadás fogja érni**, amelyet jobb költségallokációval **el lehetett volna kerülni**.

76% szerint a kollégák csak **akkor vonják be** az IT biztonságot a projektekbe, ha a **tervezési szakasz befejeződött**.

Mihály Zala

Partner | Head of Technology Consulting and Cybersecurity

Ernst & Young Tanácsadó Kft.