A vállalati ellenálló képesség növelése a szervezeti kultúra és a kiberhigiénia fejlesztésével

Szolnoki Éva, biztonsági vezető

Dátum: 2021.09.25

Magyar Energetikai és Közmű-szabályozási Hivatal

Tiszta energia, fenntartható környezet

Magyar Energetikai és Közmű-szabályozási Hivatal

1487 engedélyes (2023)

18 millió felhasználói szerződés (2022)

37 000 engedélyesi munkavállaló (2022)

12 000 milliárd Ft engedélyesi árbevétel (N°, 2021)

Engedélyesek száma	1 487 darab
Felhasználók száma (2022)	18 311 ezer darab
engedélyesek éves átlagos statisztikai létszáma (2022)	37 134 fő
Értékesítés nettó árbevétele, előzetes adat (2021)	12 022 Mrd ft

AIAIAIAIAIAIAIAIAIAIAIAIAIAIAIAIAIAI

A generatív mesterséges intelligencia (továbbiakban AI vagy AI technológia) egy mesterséges intelligencia technológia, amely különféle típusú tartalmakat, például szöveget, képeket, hangot és szintetikus adatokat képes előállítani.

A vállalatok, a saját kollégáink olyan mesterséges intelligencia által vezérelt eszközöket használnak, mint a ChatGPT és a Bard, amelyek korábbi szövegek vagy beszélgetések alapján „életszerű szöveget” generálhatnak.

Az AI technológia vállalati környezetben való használatához kapcsolódó biztonsági kockázatok

1. Érzékeny munkahelyi információk nyilvánosságra hozatala

A Samsung mérnökei ÉS a forráskód esete

2. Biztonsági rés az AI-eszközökben?

2023 március: az OpenAI offline állapotba kapcsolta a ChatGPT-t, hogy kijavítsa a chatbot nyílt forráskódú könyvtárának egy újonnan létrehozott beszélgetés első üzenete is látható volt valaki más csevegési előzményeiben, ha mindkét felhasználó körülbelül egy időben volt aktív

3. Adattorzítás és -lopás

Az AI technológiai eszközöket hatalmas mennyiségű adattal kell ellátni, hogy megfelelően működjenek. Mi történik, ha az AI manipulálása céljából rosszindulatú információkat juttatnak a képzési adatkészletbe?

4. Compliance – jogkövetkezmények

- Helytelen válaszok (az ügyfelek félrevezetése, a vállalkozás jóhírneve stb.)
- Adatszivárgás (személyes adatok, GDPR, pénzbírság stb.)
- Elfogultság (az AI-modellek válaszai időnként faji, nemi vagy egyéb elfogultságot mutatnak, ami sértheti a diszkriminációellenes törvényeket)
- A szellemi tulajdonra és a szerzői jogra vonatkozó törvények megsértése (A szerzői jog által védett művek hivatkozás nélkül való felhasználása)
- A chatbot használatára vonatkozó törvények (az ügyfelek előzetes tájékoztatásának elmaradása)
- Adatvédelem (A vállalatok érzékeny információinak nyilvánosságra hozatala sértheti az adatvédelmi törvényeket)

Bevált biztonsági gyakorlatok AI-eszközök alkalmazásakor

1. Osztályozzuk, anonimizáljuk és titkosítsuk az adatokat mielőtt a chatbotoknak továbbítanák vagy AI-modellek betanítására használnák fel

2. Képezzük a munkatársainkat

a mesterséges intelligenciával kapcsolatos biztonsági kockázatokról,

(legkritikusabb védelmi intézkedés!)

3. Végezzünk biztonsági auditokat és rendszeres penetrációs teszteket (biztonsági rések azonosítása az éles üzem előtt)

Bevált biztonsági gyakorlatok AI-eszközök alkalmazásakor

4. Szabályozzuk az alkalmazottak hozzáférését az érzékeny munkaadatokhoz (szigorú jogosultságkezelés, többfaktoros hitelesítés)

5. Biztosítsuk a mögöttes hálózatok és infrastruktúra biztonságos működését (dedikált hálózati szegmensen, a legjobb ☺ felhőszolgáltatóval)

6. A jogi háttér folyamatos figyelemmel kísérése, a beszállítók rendszeres ellenőrzése (harmadik fél által használt AI rendszer biztonsága?)

A „Szabályzat”

…amely felvázolja ChatGPT használatával kapcsolatos felelősséget, tisztázza a belső használatot és a külső szolgáltatások igénybevételét:

1. Definiálni a terminológiát

- ChatGPT? / generatív mesterséges intelligencia? / LLM? / másodpilóta (copilot)? / társtanácsadó?

2. Tiltás helyett egyértelmű iránymutatások

- a tiltás versenyhátrányhoz vezethet,
- pontos definíciók, hogy az alkalmazottak mit tehetnek és mit nem, ha az AI-jal kísérletezgetnek,
- a megértés segítése és a felelősség meghatározása,
- a különleges óvintézkedések betartásának fontossága

A munkatársak képzése az AI használat biztonsági kockázatairól - Érzékenyítés és tudatosítás

- A munkatársak képzése a legkritikusabb védelmi intézkedés az AI technológiával kapcsolatos kibertámadások kockázatának csökkentésére.
- A szervezeteknek nem elég egy AI biztonsági szabályzatot kidolgozniuk, el kell érniük, hogy a munkatársak megértsék, hogy miért keletkezett számos új szabály, amit be kell tartaniuk.
- Bár a használattal kapcsolatos sajátosságok szervezetenként eltérőek lehetnek, az általánosan bevált gyakorlat szerint folyamatos emberi felügyelet mellett alkalmazható biztonságosan: a kollégáknak át kell tekinteniük és szerkeszteniük kell mindent, amit az AI-eszközök hoznak létre.
- A képzés során a kollégáknak el kell sajátítaniuk, hogy konkrétan milyen adatok szerepeltethetők a chatbotoknak szóló lekérdezésekben és mi nem megengedett. Például a fejlesztők soha ne töltsenek be szellemi tulajdont, szerzői joggal védett anyagokat, személyazonosításra alkalmas adatokat vagy PHI-t az AI-eszközökbe.
- Sőt a képzés végére a kollégáknak el kell jutniuk odáig, hogy a neten található, a munkájukat segítő alkalmazások közül melyek működnek AI-alapon.
- Ne osszanak meg a ChatGPT-vel olyasmit, amit nem osztanának meg közösségimédia-profilon. (Néha a legjobb, ha magunkban tarjuk a dolgokat...)

Köszönöm a figyelmet!

Magyar Energetikai és Közmű-szabályozási Hivatal

Tiszta energia, fenntartható környezet