Ernst & Young Kft.
Ernst & Young Ltd.
H-1132 Budapest Váci út 20.
1399 Budapest 62. Pf.632, Hungary

Tel: +36 1 451 8100
Fax: +36 1 451 8199
www.ey.com/hu
Cg. 01-09-267553

Bernáth Dániel

Rohamosan növekvő csalás kockázatok az AI és digitalizáció fejlődésének csúcspontjain 1. rész

A generatív mesterséges intelligencia (GenAI) új korszakot nyitott a technológiai innovációban, számos üzleti lehetőséget kínálhat, de egyben új kihívásokat is teremthet a csalásmegelőzésben érdekelt szakemberek számára. Az AI által kínált lehetőségek mellett a rosszindulatú szereplők által létrehozott visszaélések is párhuzamosan fejlődnek, így komoly veszélyt jelenthetnek többek közt a digitális biztonságra és a vállalati integritásra.

I. Új mérföldkő a csalások tipológiájában - üzenet a CEO-tól

Számos technológiai fejlesztést és alkalmazási lehetőséget látunk megjelenni az üzleti világban. Ezen belül a generatív mesterséges intelligencia (genAI), amely képes önállóan adatokból, parancsra szövegeket, képeket, hanganyagokat és videókat létrehozni, különleges jelentőséggel bír. Ugyanakkor ezek az előnyök magukkal hozzák a csalások fejlesztésének lehetőségét is. A deepfake technológia olyan valósághű videókat képes létrehozni, amelyekben a szereplők arca, hangja és gesztusai szinte tökéletesen utánozhatók. Ez a technológia lehetővé teszi a csalók számára, hogy olyan személyeket utánozzanak, akiknek nagy befolyása van egy szervezeten belül, mint például az ügyvezető vagy a pénzügyi igazgató. A nemrégiben megtörtént hongkongi deepfake csalás[1], ahol egy multinacionális cég több mint 200 millió hongkongi dollárt veszített egy megjátszott, meghamisított videókonferencia miatt, csak egy példa arra, hogy milyen súlyos kockázatokat rejthetnek ezek a technológiák.

[1] https://www.scmp.com/news/hong-kong/law-and-crime/article/3250851/everyone-looked-real-multinational-firms-hong-kong-office-loses-hk200-million-after-scammers-stage

A fenti deepfake csalás-séma egyértelműen a „klasszikus” CEO-üzenet csalás kategóriába tartozik és kiemelendő, hogy a technológia nemcsak a videóüzenetek manipulációjában, de az elektronikus levélváltások esetében is segítheti a csalókat abban, hogy megtévesztően valósághű üzeneteket generáljanak, amelyekkel befolyásolhatják a cégek döntéshozóit. A csalók képesek olyan leveleket létrehozni, amelyekben a cégvezetők személyes stílusa és nyelvezete tökéletesen utánozható. Ez azt jelenti, hogy a csalóknak lehetőségük van arra, hogy a cég alkalmazottait meggyőzzék arról, hogy pénzt utaljanak át egy adott számlára, vagy érzékeny információkat osszanak meg.

A deepfake videók felismerése érdekében figyelni lehet néhány jellemző jelre, amelyek arra utalhatnak, hogy a videó manipulált:

- Ajakmozgás és hang szinkronizációja: A beszélő személy ajkainak mozgása nincs összhangban a hallható hanggal.
- Szemek viselkedése: A szemek tükröződése vagy a tekintet iránya nem stimmelhet, mintha a két szem különböző dolgokra nézne.
- Arcvonások: A bőr textúrája, az arcvonások vagy a mimika természetellenesnek tűnhet.
- Háttérzaj és beszéd: A háttérzaj digitális torzulása vagy a beszéd furcsa kiejtése, valamint a szavak értelmetlen használata is jel lehet.

Ezek a jelek segíthetnek a deepfake videók felismerésében, de fontos megjegyezni, hogy a technológia folyamatosan fejlődik, és egyre nehezebb lehet a manipulált tartalmak azonosítása. A csalások kiszűrését segíthetik a különböző deepfake-detektáló szoftverek, amelyeket már alkalmaznak különböző bűnüldözési szervek, mint például a dél-koreai rendőrség[2].

Természetesen ezen technológiák más csalásokat is hathatósan tudnak támogatni, például különböző zsaroló-levelek, hatóságok megszemélyesítése vagy románc-csalások formájában, de a legnagyobb pénzügyi kár a céges vezetők megszemélyesítésében rejlik.

[2] https://www.koreaherald.com/view.php?ud=20240305050557

II. Könnyebb lesz a dokumentumok hamisítása

Az AI robbanásszerű fejlődésének egy másik jelentős kockázati következményének tekinthető a hivatalos dokumentumok hamisítása, módosítása és a velük való visszaélések hatékonyabbá tétele. A jelenlegi technológia képes arra, hogy nagy számban, alacsony költségen autentikusnak tűnő igazolvány-másolatokat generáljon, amelyek megtévesztésig hasonló változatai a hivatalos verzióknak.

Ennek a kockázatnak az egyik legjobban kitett piaci és állami szereplői között a bankok és a különböző pénzügyi intézetek szerepelnek. A személyazonosságot vagy vagyonforrást igazoló dokumentumok fontos részei a pénzmosás-megelőzés folyamatoknak, mivel ebben a szakaszban a legkönnyebb tetten érni az illegális tevékenységet és a pénzügyi szereplők jelentős erőforrásokat biztosítanak a folyamat prudens lefolytatására. A könnyen kivitelezhető, olcsó hamisítási lehetőségek megjelenésével a bankoknak és más olyan szolgáltatóknak, akiket kötelez a pénzmosás-megelőzési törvény, elkerülhetetlenül fejleszteniük kell a belső védelmi vonalaikat és felkészülni arra, hogy egyre több hamisított dokumentummal fognak találkozni. Ezekre a KYC (Know Your Customer) folyamatokra a hamisított dokumentumokon kívül az írás első részében tárgyalt deepfake alkalmazások is veszélyt jelentenek, mivel a digitális azonosításoknál alkalmazott „élősségi" teszteken is bevethető[3].

Egy friss hír szerint[4] volt olyan eset, hogy az AI által generált hamis személyazonosságokat már 15 dollárért árulták, és képesek voltak átmenni a kriptovaluta-tőzsdék KYC ellenőrzésein. Ez azt a veszélyforrást is jelenti, hogy különböző csoportosulások, meglátva az ebben rejlő hasznot, szolgáltatóként üzérkedjenek, így segítve a különböző illegális tevékenységeket (Fraud-as-a service).

[3] https://cointelegraph.com/news/binance-rise-in-deepfake-customer-checks-verification
[4] https://cointelegraph.com/news/ai-generated-fake-ids-pass-crypto-exchange-kyc-onlyfake

1. ábra: Hamis ausztrál útlevél, amely az egykori amerikai elnök, Donald Trump adatait használja. Forrás: Telegram

A pénzmosás-megelőzés elősegítése mellett a kép-generáló technológiák több más csalást, illegális tevékenységet is támogathatnak, mint például a fiktív számlák készítése, szankció-megkerülés és embercsempészet elősegítése.

A cikkünk következő, második részében újabb kockázati elemeket mutatunk be, illetve csalási példákat hozunk a közelmúltból, amelyekkel párhuzamot tudunk vonni a jelenlegi üzleti környezettel és az abból fakadó veszélyekkel. Továbbá olyan példákról, megoldásokról írunk, amelyek segítségével fel lehet készülni az AI csalások általi kihívásokra. Érintenénk, hogy érdemes elkezdeni a kockázati feltérképezést a szervezetben,

Building a better working world

adatok elérhetőségének elemzését, kiberbiztonsági szempontok mérlegelését, illetve más megelőzést segítő kezdeményezések bemutatását célozzuk meg.