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 2. rész

A mesterséges intelligencia és a digitalizáció által nyújtott új lehetőségek mellett a csalások és visszaélések kockázata is növekszik, amint azt a cikksorozat első részében került kifejtésre. A második rész további kockázatokra hívja fel a figyelmet, amely az „AI-őrület" általi veszélyekből eredhet. Emellett stratégiákat és megoldásokat is felvázolunk a szervezetek számára, hogy felkészülhessenek az AI csalások elleni harcra, kitérve a kockázatkezelésre, adatbiztonságra és kiberbiztonsági intézkedésekre, amelyek kulcsfontosságúak a digitális kor veszélyeinek megelőzésében.

I. AI startup-ok kockázatai

Az AI forradalma óriási potenciált és növekedést rejt magában, illetve a piaci részedését 2027-re 407 milliárd dollárra teszik az előrejelzések[1]. Az AI startup-ok számának hatalmas növekedése[2] pedig a gyors növekedés és a nagy pénzügyi nyomás okán számos csalási kockázatot rejthetnek. Párhuzam vonható az olyan nagy botrányokkal, ahol olyan innovatív termékeket, megoldásokat kínáló cégek voltak érintettek, amelyek egy nagy technológiai felhajtás csúcsát lovagolták meg, mint például a hamis egészségügyi megoldásokat ígérő Theranos[3] vagy az ügyfelei pénzét elsikkasztó FTX[4].

A fenti példáknál közös nevező volt, hogy a befektetők nem végeztek kellő átvilágítást, kutatómunkát, amellyel feltudták volna mérni a kockázatokat és inkább a gyors meggazdagodás reményében kötötték meg a fenti

[1] https://www.forbes.com/advisor/business/ai-statistics
[2] https://www.visualcapitalist.com/sp/global-ai-investment/
[3] https://www.nytimes.com/2022/11/18/technology/elizabeth-holmes-sentence-theranos.html
[4] https://edition.cnn.com/2023/11/02/business/ftx-sbf-fraud-trial-verdict/index.html

aktorokkal üzleti megállapodásaikat. Az új AI startup-oknál ez a veszély is fennállhat, így fontos a kellő kockázatmenedzsment megfelelő alkalmazása. Ez a típusú körültekintés nem csak a befektetőkre vonatkozhat, de azon piaci szereplőkre is, akik új beszállítókat, szolgáltatókat keresnek ahhoz, hogy az AI adta lehetőségeket a legjobban ki tudják aknázni.

II. Megelőzés és védelem: Kulcsfontosságú a felkészülés és az adatvédelem

A fentiekben felsorolt kockázatok elhárítására, enyhítésére kész, működő megoldást találni komplex, nehéz feladatnak ígérkezik, de törekvések rá már körvonalazódnak. Mind a közvélemény, mind különböző kormányzati szervek, non-profit szervezetek hangot adnak egy olyan igényre, amely az AI-ban rejlő veszélyek megelőzését irányzó szabályozási környezet létrehozásában kapna formát. Egyes szervezetek abban látják a megoldást, hogy úgynevezett "digitális vízjel" technológiát alkalmazzanak, amely lehetővé tenné a mesterséges intelligencia által létrehozott képek, videók és szövegek nyomon követését. De amíg ezek a szabályrendszerek nem alakulnak ki, addig is a vállalatoknak, szervezeteknek proaktívan szükséges tenni annak érdekében, hogy megelőzzék az ezzel kapcsolatos visszaéléseket. Pár megelőzést segítő hasznos kezdeményezést, ötletet felsorolunk, amely jó kiindulópontként működhet:

Kockázatok feltérképezése

Át kell tekinteni a szervezetben azokat a folyamatokat, amelyek a legjobban ki vannak téve a digitális visszaéléseknek. Érdemes egy kockázati felmérést készíteni (vagy frissíteni a meglévőt), amely végig járja, hol vannak olyan pontok, ahol például email formájában történnek jóváhagyások, nincsenek kettős aláírási kötelezettségek vagy más nem-személyes üzleti interakciók zajlanak.

Adatvédelem és a nyilvános adatok feltérképezése

Fontos megjegyezni, hogy egy AI-csalás (legyen az deepfake, vagy szövegalapú) akkor működik igazán hitelesen, ha a megszemélyesített személyről (például: ügyvezető), üzleti témáról (üzleti titok, átutalási folyamat) minél több adattal rendelkezik a csaló. Az az ügyvezető, vagy felső vezető, akiről több nyilvános média-megjelenés, social média poszt van sokkal jobban kitett a kérdéses csalásoknak, mivel az AI algoritmus

így több tanuló anyagot tud felhasználni a megszemélyesítés tökéletesítésére. Ugyanez igaz az üzleti dokumentumok elérhetőségére is, amelyek esetében nem csak a digitális verziókat kell kellő védelemmel ellátni, hanem a fizikai verziókat is. Nem elhanyagolható a szervezet iratmegsemmisítési protokolljainak átnézése sem, ha minden kockázatot figyelembe veszünk.

Kiberbiztonság

A cikkben taglalt csalások megelőzésére, adatvédelem fenttartására kritikus elemként kell tekinteni az IT biztonságra és a kibertámadások megelőzésére. Érdemes biztonsági szakemberekkel közösen áttekinteni a kockázatokat és frissíteni a protokollokat. Aktualitásként megemlítendő a NIS2 keretrendszer alkalmazása, amely nem csak a szabályozásban érintett ágazatszereplőknek lehet hasznos[5].

Oktatás

A szervezet munkavállalóiban, üzleti partnereiben tudatosítani kell az AI visszaélések tényét, rendszeres oktatásokon vagy információ közlő leveleken keresztül. Továbbá érdemes a belső védelmi vonalban szereplő személyek továbbképzése olyan témákban, mint az AI, digitális biztonság és más újkori technológia innovációk.

Átvilágítás

Javasolt a szervezet átvilágítási folyamatait frissíteni, új kezdeményezéseket, megoldásokat keresni, amely hatékonyan támogatják a kockázatfelmérést. Legyen szó egy potenciális új szállító háttérinformációinak feltérképezéséről és megerősítéséről vagy egy új munkavállaló integritás-ellenőrzéséről.

III. Összegzés

A GenAI jelentős előrelépést jelent a technológiai innovációban, de a csalási kockázatok kezelése érdekében proaktív megközelítésre van szükség. AI technológia révén hitelesen és egyre könnyebben utánozhatók személyek, ami veszélyeztetheti a vállalatok integritását és sikeresen manipulálhatja a döntéshozókat, az így

[5] https://www.ey.com/hu_hu/consulting/hogyan-felelhet-meg-a-nis2-iranyelvnek

végrehajtott visszaélések és csalások felderítése egyre összetettebb feladat lehet. A szervezetek számára a kockázatok felmérése, adatvédelem hangsúlyozása, a folyamatos oktatás, a biztonsági protokollok fejlesztése és a kockázatkezelési stratégiák alkalmazása elengedhetetlen a digitális világ biztonságának fenntartásához és a gazdasági csalások megelőzéséhez.