Csizmazia-Darab István: akár szakértők is bedőlhetnek, az AI miatt sosem volt gyorsabb és olcsóbb a kibertámadás

Az AI eltörölte a korábbi árulkodó jeleket, a csalók személyre szabott üzenetekkel is bárkit megtéveszthetnek. A kiberbiztonsági szakértő szerint a hangklónozás és a deepfake új korszakot nyitott.

Gábor János | 2026. július 3.

A mesterséges intelligencia elsősorban nem új típusú kiberfenyegetéseket hoz, hanem a korábbi támadó módszereket teszi gyorsabbá, olcsóbbá és minden eddiginél hitelesebbé. Az adathalászat, a deepfake-videók és a hangklónozás, a hamis weboldalak vagy a személyre szabott megtévesztési kísérletek ma már olyan szintre fejlődtek, hogy sokszor a legóvatosabb felhasználók, sőt, akár szakértők számára is nehezen, vagy nem ismerhetők fel időben.

> **A korábbi nagy incidensek azt mutatják, hogy egyetlen figyelmetlen döntés is komoly következményekkel járhat: bizalmas adatok kerülhetnek illetéktelen kezekbe, és akár több tízmilliós károk keletkezhetnek.**

Csizmazia-Darab István az AIToday.hu-nak adott interjúban részletesen beszélt napjaink kiberfenyegetéseiről, az AI által támogatott csalások hátborzongató hatékonyságáról, a magánszemélyek és vállalatok megnövekedett kockázatairól és káreseményeiről, valamint arról is, hogy milyen alapvető lépésekkel lehet csökkenteni a támadások esélyét. A kiberbiztonsági szakértő az *ESET* termékeinek hazai forgalmazója, a *Sicontact Kft* által készített friss hazai kutatás eredményeit is bemutatta: a riport szerint a magyarok közel kétharmada használ AI-t munkacélra, de az ötödét sem éri el azon cégek aránya, ahol létezik erre vonatkozó szabályozás vagy oktatás.

— Az AI inkább új támadási formákat hoz, vagy csak a régi trükkök lettek hatékonyabbak?

— Az AI elsősorban a régi trükköket teszi nagyságrendekkel hatékonyabbá, hitelesebbé és gyorsabbá. A mai legnagyobb AI-hoz köthető kiberbiztonsági kockázatok a felhasználóknál főleg az adathalászat, a deepfake-es megtévesztés, a hangklónozás, a hamis weboldalak és a személyre szabott social engineering, vagyis a célszemély érzelmi befolyásolása köré épülnek.

> **Veszélyesebbek is a régi csalásokhoz képest, mert korábban a nyelvtanilag helytelen, tört magyarságú, sablonos levelek nagyon árulkodóak voltak.**

Az AI segítségével azonban ma már szinte tökéletes, kontextushoz illő, nyelvtanilag gyakran hibátlan, hihetőnek látszó és személyre szabott adathalász üzenetek generálhatók tömegesen, automatizálhatóan, olcsón, gyakorlatilag bármilyen nyelven. Ugyanakkor megjelentek újszerű elemek is, mint például a captcha („nem vagyok robot") feladványok automatizált kijátszása, az eszközeinken futó programok sebezhetőségeinek tömeges és villámgyors felkutatása vagy olyan eddig nem látott támadások, mint az ESET által felfedezett PromptLock: az első olyan zsarolóvírus, amely mesterséges intelligenciát használ a gépenként egyedi támadó kód generálására.

— Melyek voltak az elmúlt időszak legkirívóbb, AI-hoz köthető kiberbiztonsági esetei, és mit mutatnak ezek a kockázati trendekről?

— Az egyik legemlékezetesebb eset a Samsung mérnökeihez köthető, akik 2023. áprilisában bizalmas forráskódokat és értekezleti anyagokat töltöttek fel a ChatGPT-be, hogy gyorsabbá és hatékonyabbá tegyék a munkát, ezáltal ezek az adatok kikerültek a cég kontrollja alól. A ChatGPT a felhasználók által megadott adatokat a modell tanítására használja, így a Samsung üzleti titkai bekerültek az OpenAI szervereire és adatbázisaiba, így

> **a vállalat számára lehetetlenné vált ezen adatok visszahívása vagy törlése.**

Az egyik legelső dokumentált esetek egyike egy brit energetikai vállalat elleni 2019-es támadás. A kiberbűnözők mesterséges intelligenciával tökéletesen lemásolták egy német vállalatvezető hangját (Deepvoice), majd telefonon felhívták a cég brit leányvállalatának igazgatóját. Az igazgató azt hitte, a valódi főnökével beszél, ezért

> **a kapott utasításra gyanútlanul elutalt 220 ezer eurót a csalók által megadott számlára.**

Az utóbbi időben egyre több hír szól az önállóan döntést hozó AI-ügynökökhöz (agent) kapcsolódó incidensekről. Az Amazon például tavaly decemberben szenvedett el egy 13 órás szolgáltatás-kiesést, amelyet a Kiro nevű AI-ügynök okozott: autonóm módon döntött arról, hogy „törli, majd újra létrehozza" a futtató környezetének egy részét, ezen felül még a saját tevékenységéről is hazudott. A PocketOS nevű cég pedig például egy több mint 30 órás leállást szenvedett el, miután a programkódolási feladatokra használt mesterséges intelligencia ügynök váratlanul törölte a teljes adatbázist.

— Hogyan ismerem fel a megtévesztésre használt mesterséges intelligenciát, például adathalász üzenetben, hamis ügyfélszolgálati megkeresésben vagy csaló telefonhívásban? Csak mert van, ami még a szakértőket is átveri...

— A felismerés egyre nehezebb, mivel az AI-generált szövegekből eltűntek a korábban jellemző helyesírási hibák. Intő jel lehet azonban a szokatlan kérés, a gyanús feladói cím, például egy @gmail.com-os cím banki üzenetnél, vagy a csalásoknál jellemző sürgetés és fenyegetés. Telefonos hívásoknál is gyanakodjunk, ha az állítólagos ügyintéző olyan bizalmas adatokra, például PIN kódra, jelszóra, számlán tárolt összegre kíváncsi, amelyeket a bankok soha nem kérdeznek meg.

> **Gyanú esetén bontsuk a vonalat, ne telepítsünk ismeretlen programot, és ne utaljuk át a pénzünket egy állítólagos biztonsági, frissen bediktált számlaszámra.**

Ellenőrzésre a független csatornán vagy hivatalos számon történő visszahívás lehet a helyes módszer. Ezenkívül több banknál is elérhető az a biztonsági funkció, amellyel a netbankon keresztül azonnal ellenőrizhetjük, hogy valóban a bank hivatalos munkatársával beszélünk-e. A Google pedig nemrég vezette be a csaló hívások elleni védelmét.

— Mennyire veszélyes ma a deepfake hang- és arcklónozás, és milyen helyzetekben tudja a legkönnyebben megtéveszteni a felhasználókat?

— A deepfake technológia rendkívül veszélyessé vált, mivel ma már akár egyetlen állóképből vagy rövid hangmintából élethű hamisítvány készíthető. A csalók a siető, felfokozott érzelmi állapotban lévő áldozatokat tudják a legkönnyebben megtéveszteni, például az „unokázós" online csalás, vagy virtuális emberrablás során, amikor a szülők látszólag a gyermekük hangján hallanak segélykiáltást és váltságdíj-követelést. Szintén hatékony ez munkahelyi környezetben, ahol a „főnök" igazinak tűnő hangján érkezik sürgős és bizalmas utasítás egy azonnali nagy összegű átutalásra.

> **De sajnos hatékony módszer az is, amikor a támadók a deepfake hang vagy videó segítségével ismert ügyfélszolgálatnak, vagy befektetési tanácsadónak adják ki magukat.**

— Hogyan néz ki egy tipikus, AI-val támogatott csalási lánc a gyakorlatban, a kapcsolatfelvételtől a pénz vagy adat megszerzéséig?

— A folyamat a profilozással, adatgyűjtéssel kezdődik: az AI segítségével választanak áldozatot, és elemzik a közösségi médiából vagy korábbi adatszivárgásokból származó információkat. Ezután következik a személyre szabott csali, a hangklónozott hívás vagy a legitimnek tűnő e-mail létrehozása. A támadó sürgetéssel és félelemkeltéssel kényszeríti az áldozatot gyors döntésre, például egy kártékony linkre való kattintásra vagy adatmegadásra. Végül a megszerzett adatokkal visszaélnek, vagy a váltságdíjat nehezen visszakövethető kriptovalutában kérik átutalni.

> **Korábban a csalók gyakran széles merítéssel, tömegesen küldözgették az üzeneteiket statisztikailag kevés sikerrel, de ma már az AI lehetővé teszi a tömeges, gyors, de mégis egyénre szabott megtévesztést, ami sokkal hatékonyabb.**

— Jellemzően milyen károkat okoznak az ilyen támadások a magánembereknek vagy cégeknek? Mondanál példákat is?

— A kibertámadások ma már komoly működési, pénzügyi és reputációs kockázatot jelentenek a cégeknek. A károk a több tízmilliós veszteségektől az érzékeny adatok - köztük egészségügyi adatok - ellopásáig terjednek. A 2024 februárjában romániai kórházakat megbénító kibertámadás például az egyik legsúlyosabb egészségügyet érintő támadás volt a világon, és az ehhez hasonló incidensek gyakorisága folyamatosan emelkedik. De vegyük sorra. Közvetlen anyagi veszteségekre jó példa egy európai diszkont-kiskereskedelmi lánc szintén 2024-es esete: egy kiberincidens miatt hatmilliárd forintos kár keletkezett,

> **vagy ott a Jaguar elleni tavaly őszi kibertámadás, amelynél az okozott kár elérte az 1025 milliárd forintot.**

Ebből a példából kiindulva: előfordulhat a cég működésének részleges vagy teljes leállása – a Jaguar esetében hat hétre állt le a teljes termelés, ezzel a globális ellátási lánc is sérült. Súlyosak továbbá a jogi és szabályozási következmények: a cégek számára az adatszivárgások elkerülhetetlen velejárója a GDPR- és felügyeleti bírság. A bűnözők gyakran értékesítik a dark weben az incidensek során ellopott adatokat, amelyeket később újabb, még pontosabban célzott támadásokhoz használnak fel – ezáltal a vállalat akaratlanul is további kockázatnak teszi ki a partnereit és az ügyfeleit.

> **A pénzügyi veszteségek és a bírságok mellett a legnagyobb kockázatot a cég jó hírnevének elvesztése jelenti.**

Ha az ügyfelek vagy a partnerek adatai kiszivárognak, az olyan mély bizalmi válságot okoz, amit utólag nagyon nehéz, drága vagy akár teljesen lehetetlen helyrehozni. Magánszemélyek esetében, banki ügyfeleknél hasonló a helyzet: a SIM-cserés csalások még mindig elterjedtek, de az identitáslopás hosszú távú bizalomvesztést és rengeteg adminisztrációs terhet okoz az áldozatnak. Az ellopott adatokat gyakran eladják, és később személyre szabott támadásoknál használják fel újra meg újra. Igen gyakori a célzott, AI által támogatott adathalászat, amikor az üzenetet pontosan a címzettre szabják, és valósnak, hihetőnek tűnik, hogy minél nagyobb eséllyel kattintson rá az áldozat. Az MNB jelentése szerint tavaly év végén átlagosan 1,5-1,8 millió forintot csaltak ki magyar áldozatoktól banki csalások révén.

— Milyen szerepe van a hamis weboldalaknak, hamis videóknak és manipulált tartalmaknak az AI-alapú támadásokban, és hogyan lehet ezeket felismerni?

— Az AI gyorsan képes legyártani megtévesztő tartalmakat, klónozott hamis weboldalakat, álprofilokat. A hamis weboldalak, például a banki vagy csomagküldő oldalak hasonmásai, a bejelentkezési adatok és kártyaadatok ellopásának fő eszközei. Az AI segítségével készített manipulált képek és videók, mondjuk egy hamis halálhír vagy a Fehér Házban meg sem történt robbantás, a pánikkeltést és a dezinformációt szolgálják, vagy befektetési csalásoknak (például hírességek arcával hirdetett ál-kriptoajánlatoknak) kölcsönöznek hamis hitelességet.

> **A felismerést ezekben az esetekben segítheti a linkek fölé vitt egérmutató, a domain név előzetes és alapos ellenőrzése, vagy speciális deepfake felismerő szoftverek használata.**

De fontos észben tartani, hogy a tudatosság ma már önmagában nem elég, hiszen a megtévesztésig hasonló tartalmakat nehéz kiszűrni, még a legóvatosabb felhasználó is könnyen tévedhet. Valódi biztonságot egy megbízható, mesterséges intelligenciát is csatasorba állító védelmi szoftver jelent, amely proaktívan védi a felhasználót: automatikusan blokkolja az adathalász kísérleteket, kiszűri a vírusokat, kártevőket és zsarolóprogramokat, védi a bankolást és garantálja a zökkenőmentes, biztonságos digitális jelenlétet.

— Miben jelent új veszélyt, ha a mesterséges intelligenciát vírusok, kártevők vagy egyéb rosszindulatú programok fejlesztésére, elrejtésére vagy terjesztésére használják? Korábban egy szakértő azt mondta nekünk, hogy technikailag bárkiből válhat hacker...

— Bár a mesterséges intelligencia és a dark weben elérhető, korlátozások nélküli AI-eszközök miatt ma már mélyebb programozói tudás nélkül is bárki képes kártékony kódokat vagy adathalász üzeneteket generálni, az ESET többrétegű védelmi rendszere például fejlett AI- és gépi tanulási technológiát használva, valós időben képes felismerni és blokkolni a mesterségesen generált mintázatokat, így automatikusan és hatékonyan garantálja a biztonságot.

— Melyek azok a felhasználói hibák, amelyeket a támadók ma a leggyakrabban kihasználnak? Nyilván nem ért hozzá mindenki - ezért firtatom tovább, hogy milyen megoldásokat javasolsz?

— Nos, a támadók ma leggyakrabban a megosztott figyelmet, a kapkodást, a gyenge vagy újrahasznált jelszavakat, valamint a kétfaktoros azonosítás hiányát használják ki. A legalapvetőbb lépések, amiket mindenkinek meg kell tennie:

Különböző jelszavak használata: soha ne használjuk ugyanazt a jelszót több oldalon. Használjunk jelszókezelő programot – így csak egyetlen mesterjelszót kell megjegyeznünk, a többit a szoftver intézi és biztonságosan tárolja.

Kétfaktoros azonosítás: kapcsoljuk be mindenhol, ahol csak lehet. Ez egy extra védelmi réteg: ha a csalók valahogy meg is szerzik a jelszavunkat, a telefonunkra érkező kód nélkül nem tudnak belépni a fiókunkba.

És amit nem lehet eleget hangsúlyozni: **óvatosság, ellenőrzés.** Ha egy e-mail vagy SMS azonnali intézkedést kér (például állítólagos banki hiba vagy csomagküldés miatt), ne kattintsunk rá reflexből! Mindig ellenőrizzük a feladót, a szöveget, a linket, és ha gyanús, ellenőrizzük le a megkeresést a feladó hivatalos csatornáin keresztül.

Bár a biztonságtudatosság nagyon fontos, az AI-támogatott támadások korában az emberi éberség önmagában nem nyújt védelmet. A hatékony védelem kulcsa a felhasználói odafigyelés és egy megbízható, intelligens biztonsági szoftver kombinációja. Az *ESET* többrétegű védelme pont ott avatkozik be, ahol az emberi figyelem lankad, vagy nem képes felismerni a csalási kísérletet. A háttérben futó proaktív védelmi modulok a mesterséges intelligenciát és gépi tanulási modellt alkalmazva proaktívan blokkolják az ilyen jellegű támadásokat, még mielőtt azok bekövetkeznének. Nem csak az ismert, hanem az újonnan megjelenő kiberfenyegetéseket is felismeri és minták alapján megállítja. A fejlett adathalászat elleni védelem, a zsarolóprogramok blokkolása, valamint a tranzakciókat titkosító biztonságos bankolás és fizetési funkcióval biztonságban intézhetjük a mindennapjainkat az interneten.

— Mi a tapasztalat: mi magyarok mennyire vagyunk hajlandóak költeni a kiberbiztonságunkra?

— A hazai kkv-k és szervezetek egy része alulértékeli a kockázatokat, és gyakran csak egy bekövetkezett incidens után hajlandóak növelni a biztonsági erőfeszítéseiket. Egy korábbi felmérés szerint bár a vezetők aggódnak a támadások miatt, 70 százalékuk elismerte, hogy nem fordítanak kellő összeget és figyelmet a kiberbiztonságra. Éppen ezért, Magyarországon elsőként készítettünk olyan egyedülálló, reprezentatív kutatást, amely a mesterséges intelligencia, az IT-biztonság és a mentális egészség összefüggéseit vizsgálta a munkavállalók körében. Ez a vizsgálat rámutatott, hogy az AI használata robbanásszerűen terjedt el a vállalatoknál, ám a céges szabályozás és irányelvek nem tartják a lépést. Miközben a dolgozók a munkafolyamataik hatékonyabbá tételére törekednek, kontrollálatlanul tölthetnek fel, akár szenzitív üzleti adatokat is a nyilvános AI chatbotokba. Ez a kontrollhiány – vagyis a shadow AI jelenség – jelentősen rontja a cégek IT-biztonsági stabilitását, és komoly adatszivárgási kockázatot jelent.

> **Bár a hazai dolgozók több mint 65 százaléka használ már AI-megoldásokat, a munkahelyek mindössze 17,6 százalékánál létezik erre vonatkozó szabályozás vagy oktatás.**

Ez a belső biztonsági rés azért is aggasztó, mert 10-ből 7 munkavállaló nem tudja kiszűrni az AI-val hamisított tartalmakat, ami közvetlen és súlyos IT-biztonsági kockázatot jelent.