Deepfake VS. biometrikus védelem – az azonosítási rendszerek új kihívása

Csordás Szilárd szerint a mesterséges intelligencia fejlődése az elmúlt években szinte észrevétlenül lépte át a sci-fi határait. A deepfake, vagyis a valósághűen manipulált képek, videók és hangfelvételek néhány éve még technológiai érdekességnek számítottak. Vicces videók, kísérleti képek és felismerhető hibák jellemezték: aránytalan arcok, természetellenes mozgások, furcsa pislogások. Az idei évre azonban a technológia szinte hibátlan szintre jutott, és ma már sokszor még a tapasztalt szakembereknek is komoly kihívást jelent megkülönböztetni az igazit a hamistól. Ez a látványos fejlődés egyszerre izgalmas és aggasztó, hiszen a valóság és a manipuláció közötti határ egyre inkább elmosódik.

A deepfake-technológiát eredetileg kreatív és ártalmatlan felhasználási célokra is szánták. Filmes trükkök, digitális szinkronizálás, történelmi felvételek helyreállítása – mind olyan terület, ahol ez az eszköz értéket teremthet. Ám ahogy sok más technológiai vívmánynál, itt is igaz: ami jóra használható, az rossz kezekben könnyen válhat eszközzé a megtévesztésre és a károkozásra. A dinamitot sem rablásokhoz találták fel, mégis hamar megjelent bűnözői eszközként is.

Ez a fejlődés új frontot nyitott a kiberbiztonságban. A biometrikus azonosítás, amely korábban a megbízhatóság szinonimája volt, mára célponttá vált. Arcfelismerő rendszerek, hangazonosítók és digitális dokumentumhitelesítések kerülhetnek veszélybe, ha a támadók elég meggyőző másolatot készítenek valakiről. Ehhez már nincs szükség különleges tudásra vagy hatalmas költségvetésre. Ma már bárki hozzáférhet olyan, sokszor felhasználóbarát eszközökhöz, amelyek néhány kattintással képesek élethű digitális hasonmást létrehozni.

FOTÓK: UNPLASH

Amikor a bizalom a gyenge pont

A támadások egyre kifinomultabbak és mind inkább építenek az emberi tényezőre. A régi típusú adathalász e-mailek helyét ma már átvehetik a személyre szabott videóhívások, ahol a másik oldalon a vezérigazgató tökéletes mása sürget egy átutalást. A hang, a mimika, a testtartás mind megegyezik a valódival, így az áldozatnak esélye sincs gyanút fogni.

Az ilyen helyzetek már nem csak külföldön fordulnak elő. Magyarországi példák is akadnak, amikor pénzügyi munkatársakat úgy vettek rá nagy összegű átutalásra, hogy a hívás a főnöküknek tűnt. A biometrikus rendszerek technológiai kijátszása mellett itt a pszichológiai manipuláció is szerepet kap: az emberek hajlamosak feltétel nélkül bízni abban, akit ismerős hangon és arccal látnak.

A kiberbűnözők, akárcsak a hagyományos hackerek, folyamatosan tesztelik a célpontok védelmi vonalait. Megvizsgálják, milyen eszközöket használ a célpont, és addig alakítják a saját módszereiket, amíg át nem jutnak a védelmen. A deepfake esetében ugyanez történik: ha tudják, milyen detektáló rendszert használ egy szervezet, a hamis tartalmat addig finomítják, amíg az át nem csúszik a szűrőn.

Versenyfutás a támadók és a védelem között

A védekezéshez ma már léteznek deepfake-detektáló algoritmusok, amelyek képesek kimutatni például a pupilla apró mozgását, a hanghullámok finom eltéréseit vagy a videó képkockáinak mikroszkopikus hibáit. Ezek az eszközök azonban nem tévedhetetlenek. Az algoritmusok tanításához sok és változatos deepfake-minta szükséges, a támadók pedig folyamatosan új trükköket találnak ki, hogy túljárjanak a rendszerek eszén.

A kiberbűnözők, akárcsak a hagyományos hackerek, folyamatosan tesztelik a célpontok védelmi vonalait.

A vállalatok számára a kihívás nem csupán az, hogy beszerezzék ezeket a megoldásokat, hanem az is, hogy hatékonyan beépítsék őket a napi működésbe. Egy valós idejű videóhívás közben például másodpercek alatt kell eldönteni, hogy a túloldalon valódi ember ül-e. Ez technológiai és szervezeti szempontból is összetett feladat, amelyre kevés helyen van felkészülés.

A technológia önmagában nem elég. A kritikus pozícióban dolgozók – például a pénzügyi döntéshozók vagy a rendszergazdák – képzése legalább ilyen fontos. Fel kell ismerniük, hogy a fenyegetés ma már nem csupán e-mailben érkezhet, hanem QR-kódba rejtve, videóként vagy akár élőnek tűnő hívás formájában is.

A hazai kiberbiztonsági közösségben egyre több szakmai fórum segít a tudatosításban. Ezek közül kiemelkedik az ITBN, Magyarország legnagyobb éves kiberbiztonsági konferenciája, amely az idei, Protect Your AI-Sensitive mottójú programjában kiemelt figyelmet szentel a deepfake-támadások és a biometrikus azonosítás kapcsolatának. A résztvevők itt nemcsak a legújabb technológiákat ismerhetik meg, hanem valós eseteken keresztül tanulhatják meg, hogyan lehet felismerni és kivédeni a manipulált tartalmakat. A rendezvényről bővebben az itbn.hu/itbn-2025 oldalon olvashatnak.

A deepfake és a biometrikus azonosítás összecsapása messze nem lezárt történet. A támadók kreativitása és a technológiai fejlődés közötti versenyfutásban a legfontosabb védelmi vonalat továbbra is a felkészült, gyanakvó és tudatos ember jelenti – összegzi gondolatait Csordás Szilárd.