Do konce příštího roku se velká část českých firem stane obětí deepfake útoku

22.2.2024 - | PROTEXT

Nejčastějším typem deepfake útoku zaměřeného na firmy bude falšování hlasu nadřízeného v telefonu.

„V oblasti odhalování kybernetických podvodů jsme vždy měli výhodu složitosti českého jazyka. Často se tak stačilo soustředit na gramatické chyby a nesmyslná slovní spojení v podvodných e-mailech, které se snažily vylákat citlivé informace či přístupové údaje. Využívání nástrojů umělé inteligence ale postupně tuto výhodu eliminuje. Zároveň se aplikace pro tvorbu deepfake stávají stále více dostupnější a jednodušší na ovládání i pro laiky. Jejich využívání tak výrazně poroste a nejpozději v příštím roce se s nějakou formou kybernetického podvodu založeného na deepfake potká každá firma,“ říká Jiří Mojžíš, expert na fraud management a technický ředitel společnosti Analytics Data Factory.

Nejčastějším typem deepfake útoku zaměřeného na firmy bude falšování hlasu nadřízeného v telefonu. Útočníci snadno naleznou potřebné kontakty například na webových stránkách a zavolají z podvrženého telefonního čísla, kde uměle vytvořený, a přitom známý hlas nadřízeného může dát příkazy například k převedení finančních prostředků nebo předání určitých informací ven z firmy. Podobně lze využít i deepfake videí v online schůzkách.

Velkou hrozbou budou i falešná firemní prohlášení, kdy se na sociálních sítích objeví deepfake video, na kterém někdo z manažerů či zaměstnanců obviňuje konkurenci, obchodní partnery, nebo například „odhaluje“ nepravdivé interní informace firmy. I když se pravost videa ihned vyvrátí, může se v rámci internetu šířit roky a výrazně poškodit pověst i fungování firmy. Podobně lze v osobní rovině útočit i přímo na zaměstnance firmy, a to vydíráním deepfake nahotou – tedy uměle vytvořenými videi či fotografiemi.

„Podobně jako se neustále zdokonalují deepfake nástroje, zdokonalují se i nástroje na jejich detekci. Přesto ale největší roli zde budou hrát zaměstnanci – jejich osvěta v problematice deepfake by měla být cílem každé firmy. Právě zaměstnanci se s deepfake podvody budou setkávat stále častěji. A pokud například na základě kombinace zfalšovaného e-mailu a telefonického požadavku ředitele firmy účetní zadá platební příkaz, je zpravidla již pozdě cokoliv řešit. Důležitá je prevence,“ říká Lukáš Benzl, ředitel a zakladatel České asociace umělé inteligence.

Z důvodu stále rostoucího nebezpečí deepfake spolupracovala společnost Analytics Data Factory úzce s Českou asociací umělé inteligence na vzniku manuálu DEEPFAKE 2024: Obranná strategie pro české firmy, který je volně dostupný ke stažení na webových stránkách asociace: https://asociace.ai/deepfake-2024/.

Deepfake je označení pro realistickou úpravu obrazu či zvuku. Využívá pokročilého počítačového zpracování dat umělou inteligencí a upraví tak například tvář osob, mimiku jejich obličeje a řeč. Lidé pak ve videu vykonávají činnosti, které ve skutečnosti nedělají, a říkají to, co nikdy nepronesli.

O společnosti Analytics Data Factory:

Analytics Data Factory je na českém trhu dodavatelem a správcem řešení postavených na analytických technologiích společnosti SAS včetně veškerého navazujícího ekosystému, jako je

hardware, operační systémy, databáze, vývojový a verzovací software, messaging infrastruktura nebo big data platformy. Analytics Data Factory se primárně specializuje na oblasti, ve kterých dle referencí poskytuje služby na špičkové úrovni. Jedná se především o analýzu dat v reálném čase, a to například v oblastech aktivního řízení vztahu se zákazníky (CRM), prevence vzniku podvodů, zpracování signálů a rozpoznávání obrazu nebo pokročilé analytiky na velkých a streamovaných datech. Mezi klienty patří Komerční banka, Česká podnikatelská pojišťovna, pojišťovna Kooperativa, Home Credit, a další. Více informací o společnosti je k dispozici na www.byadf.cz.

https://www.ceskenoviny.cz/tiskove/zpravy/experti-do-konce-pristiho-roku-se-velka-cast-ceskych-firem-stane-obeti-deepfake-utoku/2482984