

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **114** ze dne **5.8.2025**

Kyberzločinci mají novou zbraň – k telefonním podvodům využívají AI boty

AI mění mnoho průmyslových odvětví a zároveň stírá hranici mezi pravdou a lží v digitálním světě. Kyberzločinci využívají generativní AI a velké jazykové modely (LLM) k ničení důvěry, takže není možné věřit ničemu, co vidíte, slyšíte nebo čtete online. AI navíc umožňuje obcházet i ty nejsložitější systémy pro ověřování identity.

Kyberzločinci mohou s pomocí AI vytvářet přesvědčivé texty, audio-vizuální materiály i interaktivní chatboty, kteří jsou schopni komunikovat s oběťmi. Precizně zfalšovat něčí hlas při telefonních podvodech nebo dokonce tvář při videohovorech už dnes není problém. Rozpoznání známé tváře nebo hlasu tedy nestačí na ověření identity. Je potřeba hledat další autentizační prvky.

AI a sociální inženýrství

Nedávno jsme měli možnost vidět přesvědčivý podvod napodobující hlas italského ministra obrany Guida Crosetta. Cílem se stalo několik významných osobností, včetně návrháře Giorgia Armaniho. Podvodníci tvrdili, že prostředky jsou nutné k propuštění rukojmích, a minimálně jedna oběť, která ministra znala, byla podvedena a poslala útočníkům významnou sumu peněz.

Podle nedávného průzkumu navíc lidé už nedokáží spolehlivě rozlišit mezi skutečnými hlasy a zvukem generovaným umělou inteligencí. Na hackerských fórech se také stále častěji diskutují komplexní kriminální telefonní systémy. Na darknetu je řada reklam, ve kterých hackerské skupiny hledají odborníky, kteří by implementovali umělou inteligenci do telefonních podvodů.

Důležitá je prevence

"Telefonní systémy využívající AI jsou dokonce již v prodeji a používají se především ke krádežím přihlašovacích údajů a ověřovacích hesel a kódů. AI boti volají potenciálním obětem a podle předem připravených scénářů získávají hesla, většinou k finančním účtům a službám," uvedl Petr Kadrmas, Security Engineer, Email Security z kyberbezpečnostní společnosti Check Point Software Technologies. "Pokročilejší platformy nabízejí flexibilní konverzační struktury, které přizpůsobují scénáře v reálném čase na základě dynamické analýzy reakcí obětí. V lednu byla například spuštěna služba, která dokazuje, jak tyto systémy dokáží plynule zvládat mnoho jazyků a zpracovávat více souběžných interakcí, čímž zvyšují možnost úspěchu ve srovnání s tradičními telefonními podvody spoléhajícími na lidské operátory. Podvodníci vytvoří jen kostru debaty, podle které AI oběť vede. A kyberzločinci avizují, že AI je schopná se odchýlit od scénáře a zvládnout neočekávané situace u jakéhokoli tématu, v jakémkoli oboru, jakémkoli jazyce a jakýmkoli hlasem."

"Tyto pokročilé AI telefonní platformy se prodávají asi za 20 000 dolarů, včetně školení a podpory, nebo je možné si je pronajmout za vstupní poplatek 500 dolarů a 1,50 dolaru za minutu. K telefonním podvodům tak nejsou potřeba ani operátoři, ani znalost technologií a schopnost tyto systémy vytvořit. Kyberzločin jako služba dává i začátečníkům do rukou obrovsky nebezpečné zbraně," dodal Kadrmas.

MEATEST spol. s r.o. - sdělení pověřence pro ochranu osobních údajů číslo **114** ze dne **5.8.2025**

V éře umělé inteligence je důležité znát rizika a při ochraně klást důraz na prevenci a využití AI technologií. Je potřeba se vymanit ze zajetých kolejí a jít za hranice tradičních metod ověřování identity. Text, hlas i video je možné věrohodně zfalšovat. Zásadní je mít přístup k nejlepším možným informacím o hrozbách a trendech a používat nástroje, které rozpoznají AI taktiky a umí na ně reagovat.

Zdroj: AVcentrum ČR