Dobrý sluha, nebo zlý pán?

UMĚLÁ INTELIGENCE MĚNÍ KYBERZLOČIN. ZATÍM SPÍŠE VE PROSPĚCH PODVODNÍKŮ

Kybernetická bezpečnost přestává být tématem pro IT specialisty a stává se každodenní realitou pro miliony lidí. Podle společnosti Visa se totiž digitální podvody šíří rychleji a ve větším měřítku než kdy dřív. Její globální tým Visa Scam Disruption odhalil během jediného roku pokusy o podvody v hodnotě přes jednu miliardu dolarů a jen v Evropě přes 220 milionů eur. Současně pomohl rozbít více než 25 tisíc podvodných obchodníků, kteří zneužívali internet k okrádání zákazníků.

Podvodníci přitom stále častěji využívají technologie, které byly původně vyvíjeny jako nástroje inovací. „Roste počet on-line podvodníků, kteří zneužívají falešné e-shopy, podvody s doručením zásilek, investiční nabídky či vydávání se za zaměstnance bank. Častěji využívají i AI, aby působili důvěryhodně," upozorňuje Petr Polák, country manager společnosti Visa pro Českou republiku. Podle dat Visa lidé, kteří nedokážou rozpoznat falešný obsah vytvořený pomocí umělé inteligence, končí jako oběti podvodů téměř pětkrát častěji. „Namísto platebních karet podvodníci stále více cílí na mezibankovní platby a bankovní účty. V Česku dosahují škody podle odhadů 7,2 miliardy korun ročně a 45 procent obětí přišlo o více než 5910 korun," doplňuje statistiky Polák.

Rozmach umělé inteligence zásadně mění podobu kybernetických útoků. Zatímco dříve byly podvodné e-maily nebo zprávy často plné jazykových chyb a působily nedůvěryhodně, dnes dokážou být téměř nerozeznatelné od legitimní komunikace. Útoky jsou přesnější, rychlejší a často i psychologicky mnohem sofistikovanější. „Největší hrozbou je phishing. Díky AI je přesvědčivější než kdy dřív. Útočníci umí napodobit banku, kolegu i rodinu. Vytvářejí deepfaky hlasu a videa. Největší problém je, že přestává být jasné, co je pravda a co lež," říká Michael Horovič, IT ředitel společnosti JRD.

Podle expertů se přitom těžiště útoků stále více přesouvá od technických zranitelností (typicky chybějících záplat např. operačního systému) k manipulaci lidí. Útočníci využívají emoce – strach, naléhavost nebo důvěru – a snaží se oběti přimět k rychlému rozhodnutí. „Útok dnes nestojí na technice, ale na manipulaci s emocemi," komentuje Horovič.

VLADIMÍR BARÁK

ÚTOKY JSOU PŘESNĚJŠÍ, RYCHLEJŠÍ A ČASTO I PSYCHOLOGICKY MNOHEM SOFISTIKOVANĚJŠÍ.

Podobně hovoří i nadnárodní poradenské společnosti. Ty často zdůrazňují, že ochrana velkých společností a jejich majetků často začíná u toho, jak zodpovědně se chovají řadoví zaměstnanci. „Pro jednotlivce na běžné denní úrovni jsou určitě největším rizikem scamy, které se šíří přes e-mail, WhatsApp nebo třeba Facebook, kde někdo předstírá identitu blízké osoby a žádá o peníze v krizové situaci," říká Petr Špiřík, partner PwC pro bezpečnost.

Právě sociální inženýrství – tedy manipulace lidí – je dnes podle bezpečnostních expertů nejrozšířenější formou kybernetických útoků. „Podvodníci se rádi vydávají za bankéře, policisty nebo investiční poradce a cílí hlavně na emoce," potvrzuje Jakub Večerka, odborník na kybernetickou bezpečnost z Raiffeisenbank.

Vedle falešných telefonátů a zpráv se stále častěji objevují také sofistikovanější techniky. Jednou z nich jsou například NFC podvody, kdy útočníci přimějí oběť k instalaci škodlivé aplikace, která následně umožní zneužití platební karty. „Oběť se domnívá, že se vzdáleně identifikuje pomocí platební karty, ve skutečnosti ale podvodníkům umožňuje v reálném čase provádět výběry z bankomatu či nákupy zboží," popisuje Jiří Poláček, odborník na prevenci platebních podvodů z MONETA Money Bank.

Telekomunikační operátoři mezitím registrují dramatický nárůst pokusů o podvody. „Každý den se kyberpodvodníci snaží prostřednictvím falešných telefonátů a zpráv získat citlivé údaje nebo peníze. Nejčastější jsou aktuálně zprávy typu ‚Ahoj mami, mám nové číslo, ztratil jsem telefon'," specifikuje Radek Šichtanc, ředitel bezpečnosti O2. Jen díky antispoofingové ochraně sítě se podle něj denně zablokuje přibližně 25 tisíc pokusů o podvržené volání (viz box).

Umělá inteligence je v tomto kontextu typickým příkladem technologie, která může sloužit oběma stranám. Bezpečnostní systémy ji využívají k analýze obrovského množství dat, odhalování podvodných

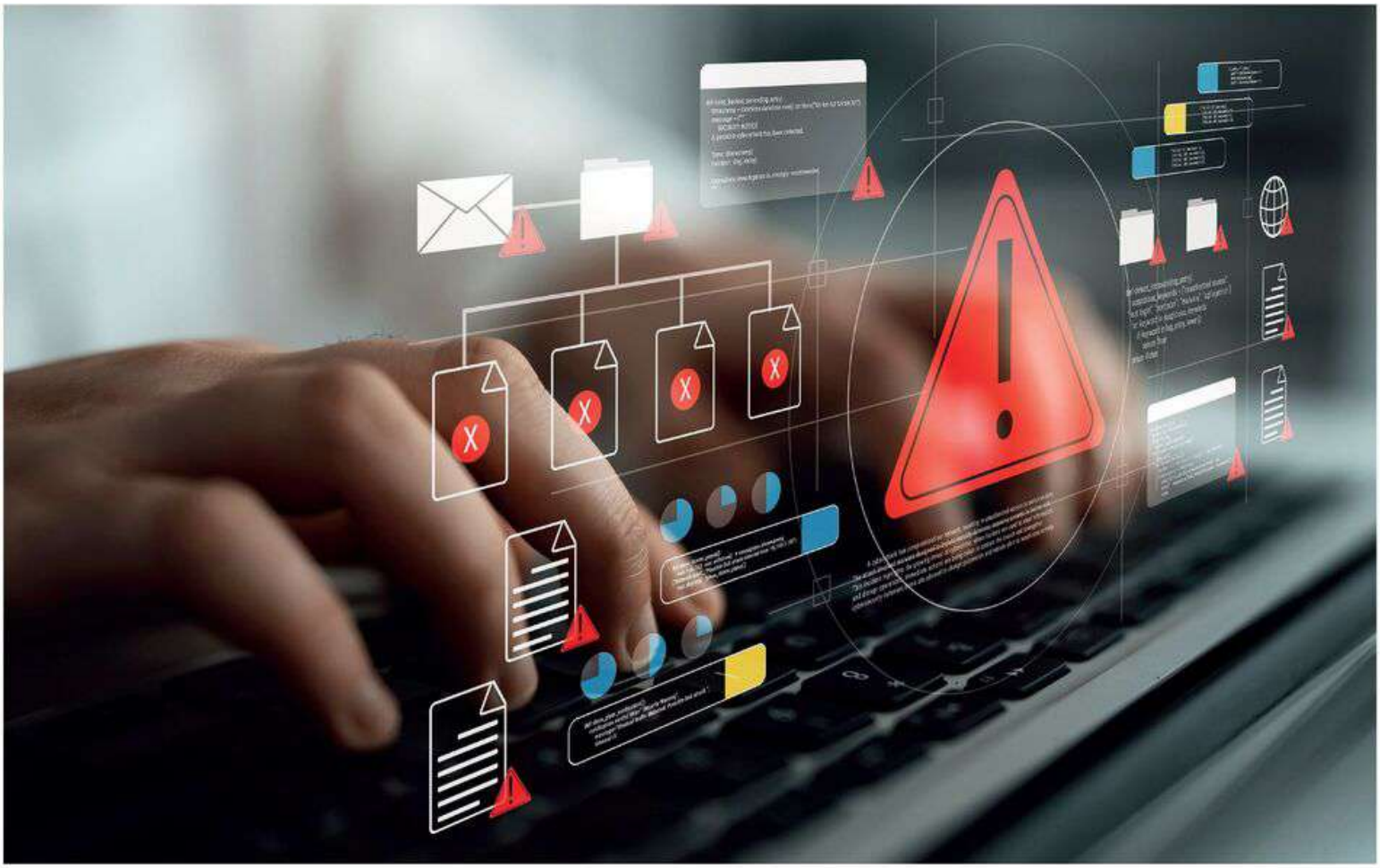

Foto: Shutterstock

vzorců a blokování podezřelých transakcí v reálném čase. Stejné nástroje ale využívají i útočníci.

Podle bezpečnostních firem se tak kybernetický prostor mění v prostředí, kde rozhoduje především rychlost reakce a schopnost rozpoznat manipulaci. „Útočníci zneužívají lidské emoce a pomocí technologií imitují například obraz nebo hlas," upozorňuje Vítězslav Pelc ze společnosti ESET.

Základní obrana přitom zůstává překvapivě „jednoduchá": obezřetnost. Experti se shodují, že většina útoků uspěje jen proto, že lidé jednají ve stresu nebo pod časovým tlakem.

„Roky platí, že hlavní je nejednat ve stresu. Vše je potřeba si ověřit a nikdy nezadávat citlivé údaje tam, kde si nejsme stoprocentně jisti, že jsme na správné stránce," říká Vladimír Borský, někdejší vyšší policejní důstojník, dnes působící na Newton University. „Vždy si velmi pečlivě vybírejte, s kým a jak komunikujete. A to nejen vy, ale i vaše děti. Pokud se vám něco nezdá, raději hovor ukončete, na podezřelý odkaz v e-mailu nebo SMS neklikejte," doplňuje radí Petr Molinek, bezpečnostní expert O2. ■

V PERMANENTNÍM OHROŽENÍ

Kybernetické útoky jsou každodenní realitou digitálního prostoru. Data operátora O2 ukazují, v jakém měřítku se podvodníci snaží dostat k citlivým údajům a penězům běžných uživatelů. V případě souhrnných statistik všech operátorů by čísla výrazně narostla.

***25 000 pokusů o podvržené telefonní hovory** je každý den zablokováno díky antispoofingové ochraně sítě.*

***5000 podezřelých SMS** denně posílají lidé na číslo 7726, kde je analyzují bezpečnostní experti.*

***50 nových podvodných domén** je díky analýze těchto zpráv denně zablokováno.*

***1,2 milionu podezřelých SMS** nahlásili lidé na číslo 7726 za rok 2025.*

***250 000 podezřelých zpráv** přišlo jen během prvních dvou měsíců letošního roku. Díky nim bezpečnostní experti zablokovali téměř 2000 podvodných domén.*

*Celkem bylo v roce 2025 zaznamenáno přibližně **7 milionů telefonátů**, které se vydávaly za jiné číslo.*

JAKÁ JSOU AKTUÁLNĚ NEJVĚTŠÍ KYBERNETICKÁ RIZIKA? JAKÁ PRAVIDLA BY MĚL BĚŽNÝ UŽIVATEL DODRŽOVAT, ABY BYLY JEHO PENÍZE A DATA V BEZPEČÍ? MŮŽE NÁM V BOJI S TZV. KYBERŠMEJDY NĚJAK POMOCI UMĚLÁ INTELIGENCE?

Michael Horovič
IT ředitel, JRD

Největší hrozbou je phishing. Díky AI je přesvědčivější než kdy dřív. Útočníci umí napodobit banku, kolegu i rodinu. Vytvářejí deepfaky hlasu a videa. Největší problém je, že přestává být jasné, co je pravda a co lež. Útok dnes nestojí na technice, ale na manipulaci.

Unikátní heslo pro každou službu. Dvoufaktorové ověřování všude, kde to jde. Ideálně přes aplikaci. Nikdy neposílat ověřovací kódy. A držet se pravidla důvěřuj, ale prověřuj. Většina útoků uspěje jen proto, že jednáme rychleji, než přemýšlíme.

AI dokáže projít obrovské množství dat a odhalit vzorce, které člověk nevidí. Umí včas zachytit podvodné kampaně i podezřelé transakce. Je to silný obranný nástroj. Jen je potřeba počítat s tím, že ji používají i útočníci.

Marie Fajstavrová
tisková mluvčí a vedoucí komunikace, Huawei Technologies CBG CZ/SK

Jako jedno z největších kybernetických rizik vnímám phishing – stále se opakující nebezpečí v podobě falešných telefonátů z banky či finančního úřadu. V době, kdy se AI stává všeobecně používaným nástrojem na práci či studium, je riziko toho, že bude podvodník úspěšný, větší než kdy jindy.

Je velmi důležité na všech svých účtech, elektronických stránkách apod. používat dvoufaktorové ověření. Dále také využívat manažera hesel, který vám dokáže vygenerovat silné heslo a bezpečně ho v sobě uložit. A v neposlední řadě je dobré mít na svých účtech a aplikacích nastavené zabezpečení pomocí biometrie (sken obličeje / otisk prstu).

AI pomáhá už nyní. Vždy když obdržíte podezřelý e-mail či telefonát, je nejlepší se AI zeptat. I já sama tuto možnost využívám. Stačí do promptu AI napsat či zkopírovat text, např.: „Přijde ti tato zpráva/číslo podezřelá/é a proč?“ Chat vám poskytne detailní vysvětlení rizika a jeho možné dopady. Zároveň mi ale přijde, že AI je spíše primárně využívána k samotnému podvodu než k obraně před ním.

Jiří Poláček
odborník na prevenci platebních podvodů, MONETA Money Bank

Setkáváme se s různými podvodnými schématy a všechny podvody mají jedno společné – sází na naše lidské slabosti, jako je strach, nepozornost, naivita či touha po penězích. Stále častěji se setkáváme s tzv. NFC podvody, kdy podvodníci přimějí oběť k instalaci malwaru, skrze který zcizí karetní údaje i PIN. Oběť se domnívá, že se vzdáleně identifikuje pomocí platební karty, ve skutečnosti ale podvodníkům umožňuje v reálném čase provádět výběry z bankomatu či nákupy zboží.

Zásadní je nejednat ukvapeně a vždy rozumět tomu, co právě dělám a proč. Pokud něčemu nerozumím, je lepší zastavit se a informace si ověřit. Své citlivé údaje je nutné si chránit a neinstalovat aplikace, u kterých si nejsem jistý, k čemu slouží.

AI pomoci může, ale obávám se, že především negativně. Se stále sofistikovanějšími AI nástroji bude pro podvodníky jednodušší, rychlejší a levnější vyrábět věrohodná manipulativní schémata, s jejichž pomocí z obětí vymámí peníze.

Petr Špiřík
partner PwC pro bezpečnost

Pro jednotlivce na běžné denní úrovni jsou určitě největším rizikem scamy, které se šíří přes e-mail, WhatsApp nebo třeba Facebook, kde buď někdo předstírá identitu blízké osoby a žádá o peníze v krizové situaci, předstírá, že je policista nebo banka, a naléhá na „převedení peněz“ do bezpečí atd.

Dlouhou dobu takové pravidlo bylo vyhnout se kradenému softwaru, ale to už je myslím vyhraná válka. Dnes bych si dával pozor na věci, které něčím vybočují z normálu – nátlak pomocí urgentní situace, netypická forma kontaktu (policie po mně většinou přece nechce, abych převáděl peníze) atd. Zároveň je vždycky dobré takovou žádost odmítnout provádět v časovém stresu – a naopak ji nezávisle ověřit.

V případě AI jde o něco, co umožňuje útočníkům jejich staré dobré triky dělat ve větší škále, rychleji, kvalitněji a levněji. Jiná rovina je ve firemním kontextu, kde se aplikace umělé inteligence do obrany stala asi největším tématem doby, ale pro jednotlivce je umělá inteligence čiré zhoršení situace a rizika.

Radek Šichtanc
ředitel bezpečnosti O2

Každý den se kyberpodvodníci snaží prostřednictvím falešných telefonátů a zpráv získat citlivé údaje nebo peníze. Díky antispoofingové ochraně sítě se denně zablokuje přibližně 25 tisíc pokusů o podvržené volání. Zákazníci zároveň každý den posílají na nahlašovací číslo 7726 asi pět tisíc podezřelých SMS, které O2 analyzuje. Na základě těchto hlášení je denně blokováno v průměru padesát nových podvodných domén. V roce 2025 lidé na číslo 7726 poslali více než 1,2 milionu podezřelých zpráv, jen za první dva měsíce letošního roku už 250 tisíc. Díky nim bezpečnostní experti zablokovali téměř dva tisíce podvodných domén.

Nejčastější jsou aktuálně zprávy typu „Ahoj mami, mám nové číslo, ztratil jsem telefon“. Celkově bylo loni zaznamenáno asi sedm milionů pokusů o spoofing.

Základem ochrany je obezřetnost: neklikat na podezřelé odkazy, nesdílet přihlašovací údaje ani kódy a vždy ověřovat neznámé nebo neobvyklé žádosti, i když přicházejí od známých kontaktů. Pomoci může také dvoufázové ověření účtů. Umělá inteligence pomáhá analyzovat podezřelé SMS a rychleji odhalovat nové podvody.

Vítězslav Pelc
tiskový mluvčí, ESET

Z hlediska běžných spotřebitelů jsou dominantní hrozbou techniky sociálního inženýrství, mj. podpořené umělou inteligencí. Útočníci zneužívají lidské emoce a pomocí technologií, které umožňují vytvářet falešný digitální obsah, imitují např. obraz, hlas a jiné. Prakticky každý je ohrožen psychologickým nátlakem, který nás má donutit k chybě – kliknutí na podvodný odkaz či instalaci škodlivého kódu.

Základem je dvoufázové ověření (2FA) u všech klíčových účtů a zdravá skepse. Nikdy nezadávejte citlivé údaje na webech, které nemají v adresním řádku ikonku zámku (protokol https), a i tehdy prověřujte důvěryhodnost zdroje. Pro bankovnictví a e-maily využívejte pouze soukromé, zabezpečené sítě, nikoli veřejné wi-fi.

AI je dvousečná zbraň. Útočníci ji sice využívají k automatizaci podvodů, ale pro obránce představuje revoluční posun. Moderní antivirová řešení díky ní fungují jako bleskový digitální imunitní systém. AI dokáže v reálném čase analyzovat miliardy dat a zablokovat i zcela nové typy škodlivého kódu nebo podvodných stránek dříve, než na ně uživatel stihne kliknout.

Vladimír Borský
vedoucí Centra rozvoje kompetencí Newton University

Jako bývalý vyšší policejní důstojník a dnes mimo jiné působící jako preventista projektu E-Bezpečí považuji za největší aktuální kybernetické riziko aktivní kyberšmejdy, kteří z lidí podvodem lákají peníze. Útočí přes falešné telefonáty, kdy se vydávají za banku, policii či jinou autoritu, příbuzného v nouzi, ale i přes falešné e-shopy, platební brány a dokonale napodobené weby známých značek. Nově často zneužívají i důvěru a vystupují jako „investiční partneři“ bank a slibují bezpečné zhodnocení peněz. Riziko roste hlavně v době silných on-line nákupů.

Základní pravidlo je jednoduché. Nejednat ve stresu, vše si ověřit a nikdy nezadávat citlivé údaje tam, kde si nejsme stoprocentně jisti, že jsme na správné stránce. Při podezřelém hovoru je vhodné zavěsit, zavolat si zpět na oficiální linku instituce a číslo zablokovat.

Umělá inteligence už dnes pomáhá odhalovat spam, podvodné zprávy i podezřelé vzorce chování. Současně ale může být zneužívána k přesvědčivějším podvodům, falešným chatbotům či cílení na zranitelné oběti. I proto je důležitá prevence a vzdělávání.

Jakub Večerka
odborník na kybernetickou bezpečnost, Raiffeisenbank

Největším rizikem je dnes velmi propracované sociální inženýrství, tedy manipulace klientů, zejména přes hovory, sociální sítě a komunikační platformy typu WhatsApp a Messenger. Kyberšmejdi se rádi vydávají za bankéře, policisty nebo investiční poradce a cílí hlavně na emoce. Vidíme však také případy, kdy ke klientům chodí i domů. Ohrožen je každý, kdo má telefon nebo přístup na internet.

Protože podvodníci dnes nejčastěji cílí na „hackování“ lidí, vhodnou obranou je zdravá nedůvěra v kohokoli, kdo se mi ozve v souvislosti s financemi. Také platí, že banka po vás nikdy nebude chtít převádět vaše finance nebo instalovat software pro vzdálený přístup.

Umělá inteligence dokáže v reálném čase analyzovat transakce nebo vyhledávat škodlivý software. Bohužel ji čím dál častěji používají i kyberšmejdi, kteří během chvíle vytvoří dokonalé kopie stránek, e-mailů nebo deepfake videa. Zároveň masově zlepšují psychologické taktiky. Ve finále je nejsilnější obranou selský rozum a pravidlo, že si veškeré kroky raději dvakrát ověřím, třeba na oficiální infolince banky nebo s rodinou.