Môžete AI zveriť firemné tajomstvá?

AI

Podľa tohtoročného zahraničného prieskumu vložila viac ako tretina zamestnancov do verejných AI nástrojov zákaznícke dáta. Firemné tajomstvá však AI zveriť môžete, ak AI beží priamo vo firme. O tom, prečo lokálna AI dáva zmysel práve teraz, sme sa rozprávali s Danielom Brnákom, IT konzultantom spoločnosti Alanata, a. s.



Daniel Brnák

FOTO: ARCHÍV

Prečo by mali firmy uvažovať o vlastnej prevádzke AI, keď sú cloudové AI služby čoraz dostupnejšie a cenovo výhodnejšie?

Subscripcie cloudových AI služieb sú dnes lacné, lebo ich poskytovatelia dotujú. Najväčšie technologické firmy podľa Financial Times investujú tento rok do infraštruktúry okolo 725 miliárd dolárov, o 77 % viac ako vlani, a skôr či neskôr to niekto zaplatí. Druhým dôvodom sú dáta. Zákaznícke konfigurácie, zmluvy pod NDA či osobné údaje do verejnej AI posielať nemožno. A tretím je dostupnosť a nezávislosť. Tento rok v júni americké exportné kontroly na takmer tri týždne odstavili prístup k najvýkonnejším modelom firmy Anthropic. V júli zas tím platformy Hugging Face pri riešení bezpečnostného incidentu narazil na to, že cloudové modely analýzu útoku odmietli, a musel siahnuť po open-weight modeli na vlastných serveroch.

Jednou z častých obáv pri lokálnej AI je kvalita a výkonnosť dostupných modelov. Dokážu dnes lokálne prevádzkované modely konkurovať najlepším komerčným cloudovým riešeniam?

Odstup je menší, než si mnohí myslia. Podľa mojich odhadov sú dnešné open-weight modely tam, kde boli najlepšie cloudové modely pred pol rokom, a s prácou s dokumentmi, programovaním či návrhom architektúry si poradia výborne. Dobrým príkladom je GLM-5.3-Flash od spoločnosti Z.ai. V augustových testoch od Artificial Analysis, ktoré hodnotili bežné pracovné úlohy a halucinácie, predbehol aj niektoré špičkové cloudové modely a vymýšľa si menej než väčšina z nich. V októbri pribudla aktualizácia populárneho modelu DeepSeek V4.1 Flash, ktorú práve testujeme. Oba modely sú navyše multimodálne, teda okrem textu rozumejú aj obrázkom, napríklad schémam, fotografiám z výroby či naskenovaným dokumentom.

Mnohé z najvýkonnejších open-weight modelov pochádzajú z Číny. Mali by firmy pri ich nasadzovaní zohľadňovať geopolitické a bezpečnostné riziká?

Z pohľadu dát nie, ak model beží lokálne. Open-weight model je len súbor, ktorý beží na firemných GPU serveroch a nepotrebuje pripojenie na internet. Je preto jedno, kto ho vyvinul, dáta firmu neopustia. Pred nasadením si však treba dať pozor najmä na licenčné podmienky a na to, či model nemá zabudované skreslenia. Geopolitické riziko je skôr v tom, že ďalšie verzie nemusia byť dostupné alebo ich zakáže regulácia či firemná politika. Preto je dobré nestavať riešenie na jedinom modeli a mať v zálohe aj modely od európskych či amerických vývojárov.

Pre aké typy firiem a organizácií má lokálna AI najväčší zmysel?

Pre každého, kto pracuje s citlivými dátami, napríklad pre banky, poisťovne, telekomunikačných operátorov, zdravotníctvo, priemysel či verejnú správu. Tam často nie je otázka, či chcú dáta poslať von, ale či vôbec smú. Na Slovensku od začiatku roka 2025 platí novela zákona o kybernetickej bezpečnosti implementujúca smernicu NIS2. Prevádzkovateľom základných služieb ukladá zodpovednosť aj za bezpečnosť dodávateľov a cloudový poskytovateľ AI je jedným z nich. Kto má AI aj dáta doma, má to výrazne jednoduchšie.

Akú technologickú infraštruktúru potrebuje firma na prevádzku vlastnej AI platformy?

Kľúčové je, aby AI bežala na rovnakej platforme ako ostatné firemné aplikácie. Ako Red Hat Premier Partner staviame na Red Hat OpenShift AI. Nové GPU servery doň jednoducho pridáme a AI sa tak stáva ďalšou aplikáciou s rovnakou správou, bezpečnosťou a monitoringom. Ak firma OpenShift nemá, GPU servery vieme rovnako pripojiť aj do existujúceho Kubernetes klastra. Pri výbere riešenia rozhoduje najmä to, aký veľký model firma potrebuje, koľko ľudí a agentov ho bude naraz používať a akú platformu už prevádzkuje.

Prečo pri budovaní AI infraštruktúry odporúčate práve technológie Red Hat?

Lebo stoja na open source. Platforma aj nástroje sú otvorené, takže zákazník nie je uzamknutý u jedného výrobcu modelov, čipov ani cloudu. Riešenie podporuje grafické akcelerátory od viacerých výrobcov a open-weight modely sa dajú vymeniť, keď príde lepší. Pri AI, kde sa trh mení čím ďalej, tým rýchlejšie, je táto flexibilita rozhodujúca.

Nie je vybudovanie a prevádzka vlastnej AI infraštruktúry pre firmy príliš nákladná? Kedy sa takáto investícia ekonomicky oplatí?

Lacné to nie je. Vstupná investícia je výrazná, výkonné GPU servery stoja aj stovky tisíc eur. A k tomu treba pripočítať prevádzku, pretože náklady na elektrinu a chladenie tiež nie sú minimálne. Celkové náklady sú však predvídateľné a nerastú s každým novým používateľom. Ten istý GPU server pritom môže súbežne slúžiť AI asistentom pre zamestnancov, agentom pre vývojárov aj automatizácii procesov, prípadne sa na ňom dá dotrénovať menší model na konkrétny účel. Na overenie konceptu (proof of concept) stačí aj hardvér do 30 000 eur. Investícia sa oplatí najmä vtedy, keď AI denne používa veľa ľudí a agentov alebo keď citlivé dáta do cloudu poslať nemožno. Príkladom je európsky fintech Revolut. Približne 2 000 jeho vývojárov od jari používa open-weight model GLM vo vlastnej réžii a firma platí desatinu toho, čo predtým za cloudové služby. A keďže zamestnanci prestali šetriť na používaní AI, dĺžka dodania zmien sa skrátila o 70 %.

Znamená lokálna prevádzka AI automaticky aj vyššiu bezpečnosť a lepšiu ochranu firemných dát?

Samotná lokálna prevádzka nestačí. Zabráni tomu, aby dáta odišli k externému poskytovateľovi, no vnútri firmy ich musia chrániť správne nastavené oprávnenia. AI agent preto vidí len to, čo smie vidieť konkrétny používateľ, alebo to, čo mu firma výslovne pridelí. Citlivé dáta ako platy či zmluvy zákazníkov tak zostanú dostupné len tým, ktorí k nim majú prístup.

KTO JE DANIEL BRNÁK

Daniel Brnák je IT konzultant v spoločnosti Alanata, a. s., s viac ako 20-ročnými skúsenosťami v oblasti informačných technológií a držiteľ certifikácie Red Hat Certified Engineer (RHCE). Venuje sa platform engineeringu, IT infraštruktúre a DevOps. Stavia moderné kontajnerové platformy a má praktické skúsenosti s nasadzovaním lokálnych jazykových modelov na GPU serveroch a s ich prepájaním s internými systémami. Vo voľnom čase experimentuje s embedded systémami a prispieva k open source projektom.

Aké nové bezpečnostné riziká prináša využívanie AI vo firemnom prostredí?

Niektoré riziká sú spoločné pre lokálnu aj cloudovú AI, napríklad takzvané halucinácie, keď AI odpovie presvedčivo, ale nesprávne. Preto má AI odpovedať vždy s odkazom na zdroj, aby si to človek mohol overiť. Ďalším rizikom je takzvaný prompt injection. Niekto do dokumentu alebo obrázka vloží text, ktorý sa snaží AI zmanipulovať, aby urobila niečo, čo nemá. Obrana je v návrhu systému. Obsah z firemných systémov musí AI brať ako dáta, nie ako príkazy. Má mať len oprávnenia, ktoré na svoju prácu nevyhnutne potrebuje, a akcie s väčším dosahom má potvrdzovať človek. Každý krok AI sa navyše zaznamenáva, takže sa dá spätne overiť, čo urobila, na základe čoho a pre koho.

Ako možno lokálnu AI bezpečne prepojiť s firemnými systémami tak, aby zamestnancom prinášala pridanú hodnotu bez ohrozenia?

AI sa k firemným systémom pripája cez integračné konektory. Cez ne číta zdrojové kódy, tickety, dokumentáciu či databázy priamo v čase otázky, takže odpovedá z aktuálnych dát. Prístup sa riadi oprávneniami používateľa alebo vlastnými oprávneniami agenta, ako som spomínal. Zápisy treba mať pod kontrolou, napríklad zmeny v kóde by mali ísť cez schvaľovací proces, kde ich potvrdí človek. Keďže model aj konektory bežia vo firme, citlivé údaje neopustia firemnú sieť.

Ak chce firma začať s vlastnou AI, aké by mali byť jej prvé kroky?

Najprv si treba ujasniť, prečo vlastne lokálnu AI chce. Či ide o citlivé dáta, ktoré nesmú opustiť firmu, o splnenie regulácie, o nezávislosť od cloudových poskytovateľov alebo o dlhodobé náklady. Potom treba zvážiť rozsah využívania, teda koľko ľudí a nástrojov bude AI používať a ako intenzívne. Od toho sa odvíja, ktoré systémy treba napojiť, aký veľký model stačí a aký hardvér je potrebné zabezpečiť. Až keď je cieľ jasný, má zmysel vybrať prvú oblasť a overiť ju v menšom rozsahu. Stavať hneď veľké riešenie pre celú firmu je finančne riskantné, pretože na začiatku sa dá len ťažko správne odhadnúť, čo firma naozaj potrebuje. Ponúkajú sa dve možnosti. Buď na prenajatom hardvéri v cloude s menej citlivými alebo so simulovanými dátami, alebo na lacnejšom vlastnom hardvéri, kde model síce pobeží, ale výkonom ani zďaleka nebude zodpovedať ostrej prevádzke.

Ako podľa vás bude vyzerať budúcnosť lokálnej AI vo firmách?

Posun už nastal. Dnes môže mať firma AI agentov napojených na lokálny model, ktorí nielen odpovedajú, ale aj samostatne pracujú, napríklad pripravujú podklady, rozpoznávajú obrázky, triedia požiadavky či píšu a testujú zmeny v kóde.

Agentovi sa dnes dá zadať cieľ a on si sám naplánuje kroky, priebežne overuje výsledky a v slučkách pokračuje, kým úlohu nedokončí. Aby to fungovalo, potrebuje dobre definované zadanie a prístup k správnym nástrojom a dátam. Tempo vývoja je pritom obrovské a stále sa zrýchľuje. Ešte pred rokom AI agent samostatne zvládol programátorskú úlohu, ktorá by človeku trvala pár hodín, dnes aj takú, na ktorú by potreboval viacero pracovných dní. Čím viac úloh budú agenti robiť, tým dôležitejšie bude, aby „digitálny kolega" bežal pod kontrolou s jasnými pravidlami, čo smie a čo nie.

V najbližších rokoch očakávam, že agenti preniknú z IT do všetkých častí firmy, či už ide o zákaznícky servis, výrobu, logistiku, právne oddelenie alebo účtovníctvo, a mimo firiem budú proaktívne pomáhať napríklad lekárom pri diagnostike či úradníkom pri administratíve. Na high-end hardvéri budú naďalej pribúdať lepšie špičkové modely a zároveň sa objavia menšie a efektívnejšie modely. Lokálna AI časom prestane byť výsadou veľkých firiem.



Súkromná AI v srdci firmy.

ILUSTRAČNÝ OBRÁZOK VYGENEROVANÝ AI

MS220182/01