

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **126** ze dne **2.12.2025**

Agentní AI v prohlížečích: Nová vrstva bezpečnostních rizik

Hlavní dodavatelé webových prohlížečů postupně integrují funkce vybavené AI, které dokáží plnit úkoly daleko přesahující tradiční rámec procházení webu – například rezervace v restauracích, objednávky ubytování či plánování schůzek. Tito inteligentní asistenti, tedy softwarové aplikace s umělou inteligencí, však zároveň otevírají zcela novou vrstvu bezpečnostních rizik. Mohou potenciálně procházet firemním prostředím, pracovat s citlivými daty a přistupovat k podnikovým aplikacím nebo síťovým zdrojům nad rámec tradičního procházení internetu.

Organizace měly si být minimálně vědomy toho, kde se agentní AI nástroje v souboru jejich uživatelských zařízení nacházejí a jak s nimi uživatelé pracují. V praxi to znamená důslednou inventarizaci firemního majetku, včetně softwaru přítomného nebo instalovaného na fyzických zařízeních. Klíčovou roli zde přitom hraje řízení prostřednictvím politik přijatelného používání (Acceptable Use Policy), které jasně stanoví, jaké aplikace mohou být instalovány a které nikoli. Současně je vhodné uplatnit technická opatření, jež omezují možnost instalace neschválených aplikací uživateli. Jen tak lze efektivně snížit riziko, že se do firemního prostředí dostanou prohlížeče rozšířené o agentní AI s nekontrolovaným přístupem k datům.

Nová kategorie hrozeb aneb co všechno může agentní AI "vidět"

Zásadní bezpečnostní problém spojený s agentní AI v prohlížeči spočívá v tom, že vše, co se odehrává v prohlížeči, může být přeneseno do místa, kde agentní AI zpracovává své požadavky. To zahrnuje nejen vyhledávací dotazy a zveřejněné informace, ale i objekty, které by jinak zůstaly pod přímou kontrolou uživatele. Patří sem soubory cookies, bezpečnostní tokeny nebo další údaje, k nimž má prohlížeč přístup. V okamžiku, kdy je agentní AI schopna s těmito daty pracovat mimo rámec zařízení uživatele, vzniká riziko neúmyslného úniku citlivých informací nebo zneužití přístupových oprávnění.

Zákaz, nebo řízené využití?

Otázka, zda by podniky měly spotřebitelské prohlížeče s umělou inteligencí zcela zakázat, nemá univerzální odpověď. Každá organizace musí zvážit vhodnost jejich použití ve svém konkrétním kontextu a provést posouzení rizik. Zatímco některé firmy mohou vidět v těchto nástrojích příležitost ke zvýšení produktivity, jiné se mohou rozhodnout pro přísné restrikce. V obou případech je nezbytné mít jasně definovaná pravidla a odpovídající technická opatření, která zajistí ochranu jak firemních dat, tak samotných uživatelů.

Podnikové prohlížeče a virtualizované prostředí

V reakci na uvedená rizika lze očekávat posun směrem k podnikovým prohlížečům a virtualizovaným řešením, která umožňují přísnou kontrolu nad akcemi prováděnými uživateli. Již dnes existují možnosti sestavit si vlastní prohlížeč ze zdrojového kódu nebo využít virtuální prohlížeče, v nichž jsou všechny informace před zpracováním a zveřejněním podrobeny přísnému filtrování a posouzení, aby bylo zajištěno jejich správné použití. Tyto přístupy umožňují organizacím minimalizovat riziko zneužití firemních aktiv a zachovat požadovanou úroveň bezpečnosti a soukromí.

MEATEST spol. s r.o. - sdělení pověřence pro ochranu osobních údajů číslo **126** ze dne **2.12.2025**

Každá firma by dnes měla být schopna sledovat a regulovat přístup svých uživatelů k internetu z firemních zařízení, detekovat zneužití dat či zdrojů a reagovat na incidenty v reálném čase. V době, kdy se webové prohlížeče proměňují v inteligentní agenty s přístupem k podnikové infrastruktuře, se tato schopnost stává klíčovou součástí moderní strategie kybernetické bezpečnosti.

AV centrum ČR