NÚKIB vydal Varování před některými produkty společnosti DeepSeek

10.7.2025 - | Národní úřad pro kybernetickou a informační bezpečnost

Na základě vydaného varování musí povinné osoby dle zákona o kybernetické bezpečnosti zohlednit hrozbu v analýze rizik a na zjištěná rizika reagovat přijetím přiměřených bezpečnostních opatření. Hrozba je hodnocena na úrovni „Vysoká“, tedy jako pravděpodobná až velmi pravděpodobná.

Současně doporučujeme i široké veřejnosti pečlivě zhodnotit použití dotčených produktů, popřípadě zvážení toho, jaké informace do nich vkládá. U tzv. zájmových osob, tedy osob, které jsou například ve vysokých politických, veřejných či rozhodovacích funkcích, doporučujeme dotčené produkty nepoužívat. Vydané varování a výše zmíněná doporučení jsou v souladu se zákonem o kybernetické bezpečnosti, který ukládá NÚKIB mj. zajišťovat prevenci v oblasti kybernetické bezpečnosti.

Obavy z možných bezpečnostních hrozeb vyplývají především z nedostatečného zabezpečení přenosu a nakládání s daty, ze sběru takových typů dat, která ve větším rozsahu mohou vést k de-anonymizaci uživatelů, a v neposlední řadě také z právního a politického prostředí Čínské lidové republiky, jemuž je společnost DeepSeek zcela podřízena.

Toto varování se nevztahuje na bezpečnostní testování, výzkum a analýzu dotčených produktů ani open-source velké jazykové modely společnosti DeepSeek, jejichž zdrojový kód je veřejně přístupný a který je provozován lokálně, bez možnosti komunikace se servery využívanými společností DeepSeek ani s jejími předchůdkyněmi, nástupnickými, mateřskými, dceřinými či přidruženými společnostmi.

„Při analýze, která vedla k tomuto varování, jsme vycházeli z kombinace vlastních zjištění a informací od našich zahraničních partnerů. Dotčené produkty společnosti DeepSeek nakládají s daty způsobem, který může představovat bezpečnostní riziko pro subjekty spadající pod zákon o kybernetické bezpečnosti. V kontextu právního prostředí Čínské lidové republiky, které umožňuje státním orgánům přístup k těmto datům, je důvod k obavám zcela oprávněný. To ostatně potvrzuje i nedávná atribuce kybernetického útoku skupiny APT31, napojené na Čínu, proti českému Ministerstvu zahraničních věcí. Ukazuje se, že Peking je připraven jednat v přímém rozporu se zájmy České republiky,“ uvedl ředitel NÚKIB Lukáš Kintr.

Plné znění varování naleznete zde a metodiku k varování zde.

Simultánně s tímto varováním také Vláda ČR dne 9. 7. 2025 schválila usnesení týkající se dotčených produktů DeepSeek, které brzy naleznete zde. Usnesením bylo členům vlády, ministerstvům a jiným ústředním orgánům státní správy uloženo, že jim podřízená ministerstva a další orgány státní správy nebudou pro výkon jejich pravomocí využívat produkty, aplikace, řešení, webové stránky a webové služby (včetně API) poskytované společností DeepSeek nebo jakoukoli její předchůdkyní, nástupnickou, mateřskou, dceřinou či přidruženou společností. Zákaz se týká užívání výše uvedeného na jakýchkoli zařízeních v majetku státu. Uložená povinnost musí být dle čl. IV odst. 4 Jednacího řádu vlády splněna do 30 dnů. Toto usnesení, stejně jako u varování Úřadu, nezahrnuje open-source velké jazykové modely (LLM) DeepSeek, jejichž celý zdrojový kód je k dispozici k nahlédnutí a analýze, v případě, že je model nasazen lokálně bez možnosti komunikovat na servery využívané společností DeepSeek.

OTÁZKY A ODPOVĚDI

Co je to varování?

Varováním Národní úřad pro kybernetickou a informační bezpečnost (dále jen NÚKIB nebo také Úřad) upozorňuje na existenci hrozby v oblasti kybernetické bezpečnosti, na kterou je nutné bezprostředně reagovat. Vztahuje se na povinné subjekty podle zákona o kybernetické bezpečnosti. Varování neznamená bezpodmínečný zákaz používání daných technických a programových prostředků, subjekty se však musí hrozbou zabývat a zohlednit ji v analýze rizik.

Dle českého právního řádu, konkrétně § 12 zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen ZKB) prostřednictvím varování NÚKIB upozorňuje na existenci hrozby v oblasti kybernetické bezpečnosti, na kterou je nutné bezprostředně reagovat. Dá se předpokládat, že hrozba se může dotýkat řady povinných subjektů podle ZKB. Ty se na základě zmíněného varování musí hrozbou dále zabývat a zohlednit ji v analýze rizik, kterou tyto subjekty v souladu s požadavky ZKB a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnost, dále jen VKB) již pravidelně provádí. Varování tedy neznamená bezpodmínečný zákaz používání daných technických a programových prostředků.

Samotné označení technických a programových prostředků určité společnosti za hrozbu, jak to NÚKIB ve svém varování učinil, znamená, že je nutné tuto hrozbu zvážit a rozhodnout o výši rizika, které z používání zmíněných technických nebo programových prostředků pro konkrétní prostředí konkrétní organizace plyne. Dovolí-li to tedy výsledky analýzy rizik, lze uvedené technické nebo programové prostředky nadále používat.

Proč varování vydáváme nyní?

NÚKIB vyhodnocuje hrozby v oblasti kybernetické bezpečnosti na základě vlastní činnosti, informací od partnerů i z dalších zdrojů. Pokud se NÚKIB dozví o určité hrozbě v oblasti kybernetické bezpečnosti, která dosahuje určité intenzity, musí na takovou hrozbu reagovat. Při vyhodnocování hrozby se vyhodnocuje řada parametrů, například rozšíření dané technologie, její využití v regulovaných systémech, možnost jejího zneužití, výrobce technologie a podobně. K reakci musí mít také dostatek podkladů. To, že NÚKIB varování vydal, znamená, že hrozba je nezanedbatelná a dosahuje určité úrovně a že existuje dostatek podkladů, aby varování mohlo být vydáno.

Koho se varování týká? Pro koho je platné?

Varování se týká především povinných subjektů dle zákona o kybernetické bezpečnosti. Konkrétně jsou to správci a provozovatelé informačních a komunikačních systémů kritické informační infrastruktury, správci a provozovatelé významných informačních systémů a správci a provozovatelé informačních systémů základních služeb, kteří jsou povinni podle § 5 VKB pro informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury, významný informační systém a informační systém základní služby provádět pravidelnou analýzu rizik, identifikovat rizika a identifikovaná rizika řídit. Na základě vyhodnocení rizik potom výše uvedené subjekty zavádějí a provádějí bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti v souladu s § 4 odst. 2 ZKB. Bezpečnostní opatření jsou blíže specifikována ve VKB. V souvislosti s řízením rizik musejí podle § 5 odst. 1 písm. h) bod 3 VKB tyto subjekty zohlednit mimo jiné i opatření podle § 11 ZKB, tedy i varování vydané podle § 12 ZKB.

Pro jiné organizace nebo fyzické osoby varování obecně závazné není. Nicméně s ohledem na charakter této hrozby doporučuje NÚKIB i těmto organizacím a osobám se hrozbou zabývat.

https://nukib.gov.cz/cs/infoservis/aktuality/2279-nukib-vydal-varovani-pred-nekterymi-produkty-spole

cnosti-deepseek