Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost
Mučednická 1125/31
616 00 Brno – Žabovřesky
IČO: 05800226
ID datové schránky: zzfnkp3

Spisová značka:
350-544/2025-E

Brno 9. července 2025

Číslo jednací:
4417/2025-NÚKIB-E/350

VAROVÁNÍ

Národní úřad pro kybernetickou a informační bezpečnost, se sídlem Mučednická 1125/31, 616 00 Brno (dále jen „Úřad“), podle § 12 odst. 1 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen „zákon o kybernetické bezpečnosti“), vydává toto

varování

před hrozbou v oblasti kybernetické bezpečnosti spočívající ve využívání produktů, aplikací, řešení, webových stránek a webových služeb, včetně aplikačního programového rozhraní, poskytovaných společností Hangzhou DeepSeek Artificial Intelligence Basic Technology Research Co., Ltd., nebo jakoukoli její předchůdkyní, nástupnickou, mateřskou, dceřinou či přidruženou společností (společně dále jen „dotčené produkty“) na zařízeních přistupujících k informačním a komunikačním systémům kritické informační infrastruktury, informačním systémům základní služby a významným informačním systémům. Toto varování se nevztahuje na bezpečnostní testování, výzkum a analýzu dotčených produktů ani open-source velké jazykové modely společnosti Hangzhou DeepSeek Artificial Intelligence Basic Technology Research Co., Ltd., jejichž celý zdrojový kód je veřejně přístupný a k analýze, v případě, že je model nasazen lokálně bez možnosti komunikovat se servery využívanými společností Hangzhou DeepSeek Artificial Intelligence Basic Technology Research Co., Ltd., nebo jakoukoli její předchůdkyní, nástupnickou, mateřskou, dceřinou či přidruženou společností.

Úřad hrozbu hodnotí na úrovni **Vysoká – Hrozba je pravděpodobná až velmi pravděpodobná**.

Orgány a osoby, které jsou povinny zavést bezpečnostní opatření podle zákona o kybernetické bezpečnosti, jsou povinny tuto hrozbu v souvislosti s řízením rizik podle § 5 odst. 1 písm. d) vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále jen „vyhláška o kybernetické bezpečnosti“), hodnotit na úrovni Vysoká – Hrozba je pravděpodobná až velmi pravděpodobná. V případě, že povinná osoba využívá v souladu s odst. 5 přílohy č. 2 vyhlášky o kybernetické bezpečnosti jinou metodu pro hodnocení rizik, je nutno tuto hrozbu hodnotit v rámci

této metody na srovnatelné úrovni, jako by tomu bylo v případě postupu podle § 5 odst. 1 písm. d) vyhlášky o kybernetické bezpečnosti.

ODŮVODNĚNÍ

1. Zákon o kybernetické bezpečnosti ve svém § 11 odst. 1 definuje opatření (úkony sloužící k ochraně před hrozbou nebo incidentem v oblasti kybernetické bezpečnosti, nebo k jejich řešení), mezi něž podle § 11 odst. 2 písm. a) zákona o kybernetické bezpečnosti patří mimo jiné i varování. Podle § 12 odst. 1 zákona o kybernetické bezpečnosti Úřad vydá varování, dozví-li se o hrozbě v oblasti kybernetické bezpečnosti.

2. Na základě skutečností zjištěných při výkonu své působnosti, doplněných o neutajované i utajované informace získané od domácích i zahraničních partnerů, dospěl Úřad k tomu, že využívání dotčených produktů tak, jak je popsáno výše ve výroku tohoto varování, představuje hrozbu v oblasti kybernetické bezpečnosti, a proto podle § 12 odst. 1 zákona o kybernetické bezpečnosti vydává toto varování.

3. K vydání tohoto varování vedla kombinace následujících poznatků a zjištění.

4. Při posuzování, zda výše uvedené dotčené produkty společnosti Hangzhou DeepSeek Artificial Intelligence Basic Technology Research Co., Ltd. (dále jen „společnost DeepSeek“) – toto však platí obecně pro posuzování kybernetické bezpečnosti jakékoli technologie – představují z pohledu kybernetické bezpečnosti pro Českou republiku hrozbu, je nutné zkoumat nejen technické aspekty těchto dotčených produktů, ale též širší kontext jejich fungování, a to včetně např. právního prostředí, z něhož dotčené produkty pochází. Úroveň důvěryhodnosti právního prostředí států má přímý dopad na důvěryhodnost společností, které jsou v nich usídleny a jsou takovým právním prostředím podřízeny. To může v některých případech zavdat zásadní důvody pro zpochybnění důvěryhodnosti i jejich samotných produktů.

5. Dotčené produkty společnosti DeepSeek byly vyvinuty a jsou dále provozovány společností DeepSeek, mající své sídlo v Čínské lidové republice (dále jen „ČLR“), jejímuž právnímu prostředí tudíž tato společnost bez výhrady podléhá. Na společnost DeepSeek se z výše uvedeného důvodu vztahují některé právní předpisy ČLR, které v kombinaci s dalšími (níže uvedenými) zjištěními jsou z pohledu bezpečnosti České republiky problematické.

6. Jedná se např. o zákon o státní bezpečnosti (国家安全法) z roku 2015, který všem čínským občanům a organizacím ukládá obecnou povinnost poskytnout pomoc státním orgánům v otázkách státní bezpečnosti. Současně pak zákon o státní zpravodajské činnosti (中华人民共和国国家情报法) z roku 2017 stanovuje ve svém čl. 7, že každý občan a organizace musí podpořit národní zpravodajskou činnost, poskytnout součinnost a spolupráci a zachovat mlčenlivost o utajovaných záležitostech, o kterých se v souvislosti s národní zpravodajskou činností dozví. Dále zákon o státní kontrašpionážní činnosti (中华人民共和国反间谍法) z roku 2014 ukládá povinnost poskytnout součinnost a informace o zahraničních klientech čínských společností v případě, že je budou státní orgány podezřívat ze špionážní činnosti, přičemž dle

jeho čl. 6 je tento zákon aplikovatelný i vůči institucím, organizacím a jednotlivcům, kteří organizují nebo financují špionážní aktivitu proti ČLR mimo její teritorium, kdy za špionáž mohou čínské orgány označit široké množství aktivit, a to vše bez možnosti nezávislého soudního přezkumu. Dalším z těchto předpisů je zákon o obchodních společnostech (中华人民共和国公司法 2013修订) z roku 2013 umožňující Komunistické straně Číny (dále jen „KSČ“) účinně ovlivňovat chod soukromých společností. Podle čl. 19 zmíněného zákona musí být totiž ve společnosti ustanovena organizace KSČ za účelem výkonu aktivit KSČ ve shodě s jejími stanovami, přičemž daná společnost musí pro tyto aktivity poskytnout nezbytné podmínky. Problematickými jsou pak i pravidla pro nahlašování zranitelností v síťových zařízeních (公安部关于印发网络产品安全漏洞管理规定的通知) z roku 2021, podle nichž mají výrobci technologií povinnost nahlašovat bezpečnostní zranitelnosti čínskému Ministerstvu průmyslu a IT (dále jen „MPIT“), a to nejpozději do dvou dnů od jejich zjištění. MPIT následně nahlašuje takovýto nález Ministerstvu státní bezpečnosti ČLR a dalším relevantním institucím, přičemž je výrobcům technologií zakázáno zveřejňovat tyto zranitelnosti nebo je nahlašovat zahraničním organizacím a jednotlivcům.

7. Výše uvedené zavdává důvodné obavy, že zájmy ČLR mohou být prostřednictvím aktivního nátlaku ze strany vlády ČLR stavěny nad zájmy uživatelů technologií společností podřízených právnímu prostředí ČLR, mezi něž se společnost DeepSeek, jakožto výrobce dotčených produktů, taktéž řadí.

8. Čínský stát navíc může skrze vlastnické podíly (tzv. Golden Shares) zasahovat do fungování a struktur mnoha formálně soukromých společností, přičemž státní dohled nad těmito společnostmi je ještě více prohlubován právě činností stranických buněk KSČ, které jsou v těchto společnostech na základě výše zmiňovaného zákona o obchodních společnostech (中华人民共和国公司法 2013修订) z roku 2013 povinně zřizovány. Poznatky partnerů Úřadu ostatně potvrzují, že KSČ ovlivňuje rozhodovací procesy např. při jmenování zaměstnanců jednotlivých společností.

9. Hlubší provázanost společnosti DeepSeek s vládou ČLR pak indikuje mimo jiné i účast Liang Wen-fenga, který je zakladatelem společnosti DeepSeek i její mateřské společnosti High-Flyer Technology, na sympoziu pořádaném premiérem ČLR Li Čchiangem. Tento závěr ostatně podporují i další (níže uvedená) fakta spojená jak se společností DeepSeek, tak také se společností High-Flyer Technology.

10. Mateřská společnost High-Flyer Technology, stejně jako obě pobočky společnosti DeepSeek ve městech Chang-čou a Peking, se nacházejí v technologicky velmi významných lokalitách. Technologický koridor ve městě Chang-čou je projektem realizovaným pod záštitou vlády ČLR, která rozvoj tohoto inovačního střediska centrálně řídí a dlouhodobě jej dotuje. To se přímo odráží i v podpoře tamních soukromých podniků zabývajících se výzkumem a vývojem umělé inteligence.

11. Dalším z indikátorů hlubšího propojení společnosti DeepSeek s vládou ČLR je skutečnost, že mateřská společnost společnosti DeepSeek – společnost High-Flyer Technology – byla v letech 2020 a 2023 označena jako národní high-tech podnik. Společnost High-Flyer Technology je tzv. hedgeovým fondem a v současné době představuje největší čínský kvantitativně řízený fond. V ČLR není možné takovýto hedgeový fond, jakým společnost High-Flyer Technology od roku 2015 je, spravovat bez schválení a kontroly ze strany KSČ.

12. V souvislosti s posuzováním bezpečnostní hrozby, kterou dotčené produkty společnosti DeepSeek pro Českou republiku představují, přitom není možné odhlédnout ani od skutečnosti, že zakladatel společnosti DeepSeek, Liang Wen-feng, byl pravděpodobně prostřednictvím svého vysokoškolského profesora, Siang Či-jü, který je prominentním expertem na umělou inteligenci, připojená vozidla a počítačové vidění, taktéž zainteresován do výzkumu technologií dvojího užití. V tomto kontextu je pak nutno upozornit, že Siang Či-jü publikoval studie a je držitelem patentů mimo jiné na téma provozu autonomních vozidel v bitevních prostorech s nepředvídatelným terénem.

13. Toto varování je vydáváno též ve světle skutečnosti, že Česká republika patří dlouhodobě k cílům čínských kybernetických státních aktérů. V posledních letech Úřad zaznamenal kampaně aktérů spojených s Ministerstvem státní bezpečnosti i armádou ČLR, které cílily jak na státní, tak soukromé subjekty, i přímo na jednotlivce na území České republiky. Realizaci těchto aktivit ze strany ČLR vůči České republice dokládá mimo jiné i škodlivá kybernetická kampaň, kterou vedla skupina APT31, jež je spojována s čínskou zpravodajskou službou Ministerstva státní bezpečnosti. Tato skupina od roku 2022 útočila na jednu z neutajovaných sítí Ministerstva zahraničních věcí České republiky. Závěry analýzy provedené Úřadem, Vojenským zpravodajstvím, Úřadem pro zahraniční styky a informace a Bezpečnostní informační službou jednoznačně ukazují, že za touto dlouhodobou škodlivou kampaní stojí ČLR a přímo skupina APT31 (známá též pod jménem Zirconium nebo Judgment Panda), která je spojována s celou řadou útoků proti politickým a jiným cílům mimo jiné též na území jiných členských států Evropské unie či Severoatlantické aliance.

14. Vzhledem k předchozím špionážním aktivitám, jednání proti národním zájmům členských států Evropské unie i Severoatlantické aliance, výše popsaným specifikům legislativy ČLR a vlivu vlády ČLR v čínských společnostech je velmi pravděpodobné, že ČLR využije možností produktů společnosti DeepSeek ke zpravodajské činnosti. Na uvedené vlivové aktivity v České republice ostatně opakovaně upozorňuje Bezpečnostní informační služba ve svých výročních zprávách.

15. Z důvodu obavy o národní bezpečnost a kvůli pochybnostem o dodržování ochrany osobních údajů přitom k 4. dubnu 2025 vydalo opatření proti produktům společnosti DeepSeek již deset států (Itálie, Nizozemí, Dánsko, Norsko, Austrálie, Kanada, Tchaj-wan, Jižní Korea, Indie a některé americké státy, např. Texas, Virginie či New York). Vzhledem ke složení této skupiny států je evidentní, že obavy v souvislosti s produkty společnosti DeepSeek nevyplývají pouze z jednotného kulturního prostředí a ani nejsou dány geografickou polohou těchto států, nýbrž se jedná o reakci následující po objektivní identifikaci a zhodnocení rizika představovaného těmito produkty. Je přitom téměř jisté, že v následujících měsících i další státy zavedou vůči produktům společnosti DeepSeek určitá opatření. V rámci těchto opatření státy přistupují

nejčastěji k zákazům či omezením na zařízeních státních či vládních zaměstnanců. V případě Itálie a Jižní Koreje však byly produkty společnosti DeepSeek odstraněny např. i z obchodů s aplikacemi, se kterými přichází do styku řadoví občané těchto států. K zákazu se uchylují i akademické instituce nebo soukromé společnosti po celém světě, a to taktéž z důvodu bezpečnosti a rizik spojených s ochranou osobních údajů.

16. Tímto varováním stanovená úroveň bezpečnostní hrozby současně vyplývá i z technické analýzy mobilní aplikace společnosti DeepSeek, kdy nashromážděné poznatky o fungování této aplikace taktéž jednoznačně podporují závěr Úřadu o nutnosti vydání tohoto varování.

17. Mobilní aplikace společnosti DeepSeek totiž téměř jistě shromažďuje veškerý obsah, který uživatel poskytne jak chatbotu, tak přidruženým službám. Dále sbírá také údaje o uživateli či konkrétním zařízení, přičemž vše je uchováváno na serverech v ČLR, kde k veškerým těmto datům a informacím mohou mít přístup čínské vládní autority. Současně přitom společnost DeepSeek nijak nespecifikuje dobu, po kterou jsou tato data na zmíněných serverech uchovávána, či zda jsou vůbec někdy mazána. Dle dostupných informací současně dochází k transferu těchto dat mimo jiné na servery společností Huawei a China Mobile – jedná se o společnosti sankcionované ze strany partnerů České republiky. V souvislosti se společností Huawei Úřad taktéž vydal varování. Existují přitom důkazy, že zmiňovaná data byla taktéž sdílena se společností ByteDance, jež vyvinula a nadále provozuje aplikaci TikTok, v souvislosti s níž Úřad v minulosti již taktéž vydal varování. Tuto informaci potvrzuje také interně provedená analýza Úřadu. Dle partnera Úřadu navíc mobilní aplikace společnosti DeepSeek odesílá data taktéž na servery spravované společností Zhejiang Taobao Network Co., Ltd., na území Ruské federace.

18. Nad rámec odůvodnění tohoto varování pak Úřad pro účely umožnění komplexního zhodnocení hrozby představované dotčenými produkty společnosti DeepSeek považuje za vhodné zmínit, že dotčené produkty společnosti DeepSeek současně též prokazatelně podléhají cenzuře ze strany vlády ČLR, a napomáhají tak k šíření pročínské propagandy. Důkazem této činnosti ze strany chatbota je doložené a prokázané zkreslování informací ve prospěch čínských politických narativů, v důsledku čehož dochází k poskytování záměrně zavádějících informací, které nemusí být na první pohled zjevně mylné. Tím může docházet k záměrnému a účelovému ovlivňování vnímání a názoru uživatelů ve prospěch ČLR. Jasným dokladem cenzurních tendencí dotčených produktů společnosti DeepSeek je např. odmítání poskytnutí informace o tom, k jakým událostem došlo na pekingském náměstí Nebeského klidu, či poskytování informací propagujících výklad KSČ ohledně nezávislosti Tchaj-wanu. Veškeré výše v tomto bodě uvedené informace dokládají, že dotčené produkty i samotná společnost DeepSeek podléhají vlivu a řízení ze strany vlády ČLR.

19. Vedle rizik spjatých s odesíláním dat představuje rovněž tato samotná mobilní aplikace bezpečnostní riziko související především s jejím používáním ze strany zaměstnanců, kteří nakládají s citlivými informacemi nebo zastávají důležité funkce. Mobilní aplikace společnosti DeepSeek totiž vykazuje mnohá bezpečnostní rizika v podobě nedostatečného zabezpečení přenosu dat a nakládání s nimi či sběru takových typů dat, která ve větších množstvích mohou

vést až k umožnění de-anonymizace konkrétních jednotlivých uživatelů. Technické analýzy verzí mobilní aplikace společnosti DeepSeek pro Android i iOS současně ukazují nedostatečné zabezpečení proti kybernetickým útokům.

20. Mobilní aplikace společnosti DeepSeek určená pro iOS sbírá široké spektrum dat o uživatelích i zařízení samotném (tzv. fingerprinting), přičemž některá z nich posílá nešifrovaně, neboť v rámci daného zařízení vypíná funkci App Transport Security, která je určena k bránění přenosu nezašifrovaných dat. Dle analýzy partnerů Úřadu dochází k vypnutí podobných ochran taktéž ve verzi této mobilní aplikace určené pro OS Android. Ačkoli separátně tato data nepředstavují zásadní riziko, po agregaci datových bodů už je možné identifikovat i konkrétního jednotlivce, což může být použito k sestavení profilů zájmových osob. Datovými body, které mobilní aplikace společnosti DeepSeek shromažďuje, jsou mimo jiné region, časová zóna, jazyk, způsob přístupu (např. skrze Wi-Fi), operační systém, model daného zařízení, model procesoru či jméno zařízení. Právě pro iOS je jméno zařízení v některých případech automaticky nastavováno jako jméno zákazníka, což je vzhledem k výše uvedenému velmi rizikové. V Zásadách ochrany osobních údajů z prosince 2024 společnost DeepSeek přitom deklaruje i sběr dat o úhozech na klávesnici a rytmu (tento údaj v aktualizovaných zásadách z února 2025 již chybí). Mobilní aplikace společnosti DeepSeek pro iOS dále také odporuje i dalším zásadám dobré praxe, neboť mimo jiné používá zastaralé metody šifrování či riskantně nakládá s šifrovacími klíči, čehož může být zneužito např. pro tzv. man-in-the-middle útoky, jejichž cílem je odposlouchávání komunikace. Všechny výše uvedené závěry potvrzuje i analýza partnerů Úřadu.

21. Dalším rizikovým faktorem u verze mobilní aplikace společnosti DeepSeek určené pro iOS je používání zastaralého šifrovacího algoritmu 3DES, opakované používání inicializačních vektorů a tzv. hardcodingu. Použití zastaralého šifrování výrazně usnadňuje a zvyšuje rychlost dešifrování dat. Šifrovací klíče přímo vložené do kódu pak zase umožňují dešifrování v reálném čase. Inicializační vektory by měly být unikátní a nepředvídatelné, přičemž právě jejich opakované používání snižuje úroveň zabezpečení.

22. V neposlední řadě je pak Úřadem jako riziko vnímána také možnost obnovy citlivých dat z mezipaměti zařízení (v databázi v mezipaměti, cached database), čehož mohou útočníci využít, a to především pokud získají fyzický přístup k zařízení. Takovýmto způsobem mohou útočníci získat přístup např. k přihlašovacím údajům a heslům.

23. V případě verze mobilní aplikace společnosti DeepSeek určené pro OS Android tato mobilní aplikace vykazuje slabou detekci rootování, což může útočníkům usnadnit skrytý přístup do celého zařízení. Rootování umožní všem uživatelským aplikacím spustit privilegované příkazy, které nejdou spustit při původní konfiguraci zařízení. Slabá detekce rootování pak vede k tomu, že nelze odhalit, pokud by došlo k přepnutí zařízení do privilegovaného režimu, jenž umožňuje přístup v podstatě ke všem funkcím zařízení. Útočníci s tímto přístupem tedy mohou obejít bezpečnostní kontroly. Rootovaná zařízení jsou proto velmi zranitelná vůči malwaru. Výše uvedené vyplývá z interní analýzy Úřadu.

24. Mobilní aplikace společnosti DeepSeek ve verzi určené pro OS Android současně postrádá vhodná opatření pro zabezpečení sítě, a je tedy velmi náchylná vůči útokům typu man-in-the--middle. Pakliže se uživatel připojí přes veřejnou Wi-Fi nebo nedůvěryhodnou síť, mohou útočníci zachytit data a manipulovat s nimi, popř. též ukrást přihlašovací údaje, osobní zprávy a platební údaje.

25. Riziková je v případě verze mobilní aplikace společnosti DeepSeek určené pro OS Android též absence ověřování certifikátů SSL, v důsledku čehož je tato aplikace zranitelná vůči falešným webům nebo neoprávněnému přístupu. Útočníci se tedy mohou vydávat za důvěryhodné servery a díky výše zmíněnému neověřování certifikátů SSL zachytit citlivé informace, jakými jsou např. přihlašovací údaje a osobní data.

26. Mobilní aplikace společnosti DeepSeek ve verzi určené pro OS Android se též vyznačuje náchylností ke zranitelnosti StrandHogg, která umožňuje škodlivým aplikacím přebírat úlohy legitimních aplikací, zobrazovat falešné přihlašovací obrazovky, a krást tak přihlašovací údaje uživatelů. Současně je tato mobilní aplikace náchylná též vůči zranitelnosti Janus, jež umožňuje útočníkům upravit APK soubor aplikace, aniž by došlo k porušení jeho digitálního podpisu, což umožňuje vložení malwaru. V neposlední řadě je pak mobilní aplikace společnosti DeepSeek ve verzi určené pro OS Android náchylná též vůči metodě označované jako tapjacking, jejímž cílem je oklamat uživatele tak, aby udělil nebezpečná oprávnění, a to překrytím neviditelných prvků uživatelského rozhraní na legitimních tlačítkách.

27. Co se webového klienta společnosti DeepSeek týče, umožňuje tento zadávat požadavky modelům na serverech v ČLR, kdy hlavní riziko ve světle výše uvedených informací nejen o právním řádu ČLR, ale též nežádoucích aktivitách ČLR vůči České republice, spočívá v odeslání vložených dat do ČLR a v přístupu k datům prohlížeče. Nutno zdůraznit, že veřejně přístupná databáze společnosti DeepSeek pro webového klienta, kterou odhalili kyberbezpečnostní analytici jen pár dní po veřejném spuštění velkého jazykového modelu R1 (dostupného též ve formě mobilní aplikace), byla nezabezpečená. Databáze tak umožňovala plnou kontrolu nad databázovými operacemi včetně možnosti přístupu k interním datům, přičemž tato databáze obsahovala více než milion řádků logů obsahujících historii chatu, tajné klíče, podrobnosti o tzv. backendu (což je aplikace sloužící pro administraci) a další vysoce citlivé informace.

28. Do rozsahu tohoto varování je současně zařazeno i aplikační programové rozhraní (API) společnosti DeepSeek, které je nástrojem integrace produktů společnosti DeepSeek do aplikací produktů třetích stran. Toto rozhraní umožňuje aplikacím posílat data modelu a získávat zpět zpracované odpovědi, a to obvykle přes http. Uvedené rozhraní je přitom ve světle výše v tomto varování uvedených skutečností velmi rizikové, neboť posílá data na servery v ČLR, přičemž nemusí být vůbec patrné, že daná aplikace třetí strany právě služby společnosti DeepSeek používá. V současné době jsou produkty společnosti DeepSeek začleněny do systémů a činností minimálně 20 čínských státních podniků v sektorech jako energetika, komunikace, finance či stavebnictví a využívají je i čínské společnosti jako Lenovo nebo Tencent. Velký jazykový model R1 je začleněn i jako součást produktů těchto společností. Strategické partnerství se společností DeepSeek přitom podepsaly již další téměř dvě desítky čínských společností působících v automobilovém průmyslu, z nichž některé tvoří tzv. sdílený

podnik (joint venture) se západními značkami. Zároveň je velmi pravděpodobné, že produkty společnosti DeepSeek budou do svých systémů implementovat i západní společnosti bez jakéhokoli obchodního napojení na ČLR, zvláště pak pokud ČLR zaujme svoji obvyklou strategii tzv. dumpingových cen, tedy prodeje pod cenou. Je velmi pravděpodobné, že právě skrze toto začlenění budou některé typy dat sdíleny i se společností DeepSeek. Zkreslování výsledků ve prospěch čínských narativů se tak bude moci propsat i do aplikací třetích stran, které nebudou pocházet z ČLR, přičemž společnost DeepSeek bude s velkou pravděpodobností shromažďovat data i touto cestou.

29. Výrok tohoto varování je nezbytně nutné vnímat tak, že dopadá mimo jiné i na mobilní zařízení, neboť právě ta jsou v řadě případů součástí informačních systémů regulovaných zákonem o kybernetické bezpečnosti nebo rozsahu řízení jejich bezpečnosti informací. Taková zařízení přistupují ke stěžejním aktivům tvořícím regulované systémy a narušení jejich bezpečnosti vede k přímému ohrožení bezpečnosti regulovaných systémů a k ohrožení řádného poskytování služby, pro kterou byly tyto systémy do regulace zařazeny. Současně však i ta zařízení, která sice nejsou součástí regulovaných systémů nebo rozsahu řízení jejich bezpečnosti informací, ale která jsou používána strategicky významnými osobami v organizacích spravujících nebo provozujících regulované systémy, mohou být terčem aktivit spočívajících ve sběru citlivých informací o těchto osobách a v pozdějším zneužití těchto informací např. k vydírání nebo jiné formě prosazování zájmů útočníků. V závislosti na charakteru a způsobu použití konkrétního zařízení a charakteru a citlivosti informací a dat, ke kterým má zařízení přístup, Úřad proto doporučuje přijmout adekvátní bezpečnostní opatření k eliminaci hrozby, na kterou toto varování upozorňuje.

30. Úřad hodnotí úroveň hrozby jako vysokou, tedy v souladu se stupnicí pro hodnocení hrozeb obsaženou v příloze č. 2 k vyhlášce o kybernetické bezpečnosti jako pravděpodobnou až velmi pravděpodobnou. Úroveň hrozby je dána především kombinací problematického sběru citlivých a velmi snadno zneužitelných informací a dat o uživatelích, nízké úrovně zabezpečení a právního prostředí, ve kterém společnost DeepSeek operuje a jímž je vázána. Současně nelze pominout skutečnost, že na problematičnost jazykového modelu upozorňují tuzemští i zahraniční partneři, přičemž mnohé státy již přijaly vůči dotčeným produktům preventivní opatření.

31. Současně Úřad doporučuje všem fyzickým osobám, jejichž data by mohla být cílem aktivit zahraničních zpravodajských služeb (tzv. zájmové osoby, tedy osoby, které jsou např. ve vysokých politických, veřejných či rozhodovacích funkcích), zvážit omezení či úplný zákaz využívání dotčených produktů společnosti DeepSeek tak, jak je uvedeno ve výroku tohoto varování.

32. Široké veřejnosti Úřad doporučuje věnovat pozornost tomu, jaké přístupy dotčené produkty společnosti DeepSeek požadují, jaká data shromažďují a jakým způsobem s nimi nakládají. Úřad obecně doporučuje instalovat a používat pouze takové aplikace, kterým jejich uživatel důvěřuje.

33. Jelikož úkolem Úřadu je dle § 22 písm. j) zákona o kybernetické bezpečnosti zajišťovat prevenci v oblasti kybernetické bezpečnosti, jejíž součástí je také poskytování informací zjištěných o hrozbách v oblasti kybernetické bezpečnosti, přičemž na základě veškerých výše uvedených informací, které dle Úřadu dokládají, že ve výrokem tohoto varování stanoveném rozsahu představují dotčené produkty společnosti DeepSeek pro Českou republiku bezpečnostní hrozbu, o níž nepostačuje veřejnost informovat běžnými způsoby preventivní činnosti Úřadu, přistoupil Úřad k vydání tohoto varování. Pravomoc Úřadu k vydání tohoto varování je dána ustanovením § 22 písm. b) zákona o kybernetické bezpečnosti.

34. Úřad na závěr upozorňuje, že v souladu s § 4 odst. 4 zákona o kybernetické bezpečnosti jsou orgány a osoby uvedené v § 3 písm. c) až f) zákona o kybernetické bezpečnosti povinny zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro jejich informační nebo komunikační systém a tyto požadavky zahrnout do smlouvy, kterou s dodavatelem uzavřou. Zohlednění požadavků vyplývajících z bezpečnostních opatření podle věty první v míře nezbytné pro splnění povinností podle zákona o kybernetické bezpečnosti nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži.

Elektronický podpis: 10.7.2025
Certifikát autora podpisu:
Jméno: Ing. Lukáš Kintr
Vydal: I.CA EU Qualified CA2/RSA 06/2022
Platnost do: 4.2.2026 13:05 +01:00

Ing. Lukáš Kintr
ředitel
Národní úřad pro kybernetickou a informační bezpečnost