Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Č.J. NEPŘIDĚLENO • BRNO • 10. ČERVENCE 2025

VERZE DOKUMENTU: 1.0

METODICKÝ MATERIÁL K VAROVÁNÍ ZE DNE 10. ČERVENCE 2025

Podpůrný materiál

Obsah

1 Úvod

Národní úřad pro kybernetickou a informační bezpečnost (dále jen „Úřad“) vydal dne 10. července 2025 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 (dále jen „varování“).

Zmíněné 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. (dále jen „společnost DeepSeek“), jejichž celý zdrojový kód je veřejně přístupný a k analýze, v případě, že je model nasazen lokálně bez možnosti komunikovat se servery využívanými společností DeepSeek nebo jakoukoli její předchůdkyní, nástupnickou, mateřskou, dceřinou či přidruženou společností.

Varování je dostupné na úřední desce Úřadu (https://nukib.gov.cz/cs/uredni-deska/).

Účelem tohoto metodického materiálu je poskytnout jeho adresátům praktické pokyny a informace související se zohledněním varování.

Adresáty tohoto metodického materiálu jsou veškeré povinné subjekty dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen „ZKB“).

> Upozornění:
>
> **Tento metodický materiál není určen pro orgány veřejné moci, na něž se vztahuje usnesení vlády ze dne 9. července 2025 č. 537.** V souvislosti se zmíněným usnesením vlády zakazujícím využívání vybraných produktů společnosti DeepSeek na zařízeních v majetku státu, které má vyšší právní sílu nežli varování Úřadu, je vydán samostatný metodický materiál.

V případě dotazů se prosím obracejte na sekretariát Národního úřadu pro kybernetickou a informační bezpečnost:

Národní úřad pro kybernetickou a informační bezpečnost
Mučednická 1125/31
616 00 Brno – Žabovřesky
E-mail: regulace@nukib.gov.cz

Upozornění:

Tento dokument slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů. Právo změny tohoto dokumentu vyhrazeno.

Informace obsažené v dokumentu se vztahují k právní úpravě účinné ke dni platnosti publikované verze dokumentu.

2 Důvody vydání varování

Na základě vlastních poznatků Úřadu i informací získaných od partnerů Úřadu bylo konstatováno, že společnost DeepSeek a s ní spjaté dotčené produkty představují pro Českou republiku bezpečnostní hrozbu, na niž je nutné prostřednictvím tohoto varování oficiálně a veřejně upozornit.

Společnost DeepSeek a s ní spjaté dotčené produkty představují bezpečnostní hrozbu pro Českou republiku zejména z následujících důvodů:

- nízké zabezpečení, které činí dotčené produkty společnosti DeepSeek zranitelnými vůči kybernetickým útokům,
- vypínání funkce App Transport Security bránící přenosu nezašifrovaných dat – v důsledku toho může dojít k identifikaci i konkrétního jednotlivce (slouží pro tzv. man-in-the-middle útoky),
- ukládání uživatelských dat na serverech v Čínské lidové republice, mimo jiné i na serverech společností Huawei a China Mobile, což jsou společnosti, které jsou sankcionovány ze strany partnerů České republiky (vůči Huawei ostatně i sama Česká republika již v minulosti vydala samostatné varování), a to včetně potenciálně citlivých dotazů a souborů nahraných do dotčených produktů společnosti DeepSeek jejími uživateli,
- shromažďování veškerého obsahu poskytnutého uživatelem dotčených produktů, stejně jako údajů o uživateli či konkrétním zařízení,
- sdílení dat se společností ByteDance (výrobce a provozovatel aplikace TikTok, v souvislosti s níž Úřad taktéž v minulosti vydal samostatné varování),
- odesílání dat na servery spravované společností Zhejiang Taobao Network Co. Ltd na území Ruské federace,
- podřízení společnosti DeepSeek čínskému právnímu řádu, který čínskému státu umožňuje invazivní přístup k datům společnosti DeepSeek a vynucení její spolupráce např. při špionážních aktivitách vůči uživatelům dotčených produktů společnosti DeepSeek,
- pravděpodobné hlubší napojení společnosti DeepSeek i její mateřské společnosti – společnosti High-Flyer Technology – na čínskou vládu,
- používání zastaralého šifrovacího algoritmu 3DES,
- možnost obnovy citlivých dat z mezipaměti zařízení,
- slabá detekce rootování u mobilní aplikace.

3 Co varování znamená pro jednotlivé subjekty

3.1 Povinné orgány nebo osoby podle § 3 písm. c) až f) ZKB

Správci nebo provozovatelé informačních a komunikačních systémů kritické informační infrastruktury, správci nebo provozovatelé významných informačních systémů a správci nebo provozovatelé informačních systémů základních služeb jsou povinni podle § 5 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále jen „VKB“) **pro informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury, významný informační systém a informační systém základní služby** identifikovat rizika, hodnotit rizika a identifikovaná rizika řídit.

V souvislosti s řízením rizik musejí podle § 5 odst. 1 písm. h) bodu 3 VKB tyto subjekty zohlednit mimo jiné i opatření podle § 11 ZKB, tedy i varování vydané podle § 12 ZKB. Na základě vydaného varování tedy musejí výše zmíněné povinné osoby v rámci zavedeného řízení rizik provést analýzu rizik, ve které zohlední hrozbu, a následně na riziko reagovat zavedením bezpečnostních opatření, která musí být v souladu s nastavenými metrikami pro akceptovatelnost rizika a hodnotou daného rizika.

Varování a s ním související povinnosti se však neuplatní na orgány veřejné moci, na něž se vztahuje usnesení vlády ze dne 9. července 2025 č. 537, které má vyšší právní sílu nežli varování Úřadu.

3.2 Povinné orgány nebo osoby podle § 3 písm. h) ZKB – poskytovatelé digitálních služeb

Poskytovatel digitální služby podle § 29 VKB zavádí bezpečnostní opatření podle prováděcího nařízení Komise (EU) 2018/151 ze dne 30. ledna 2018. Toto nařízení poskytovateli digitální služby ukládá pro informační systém nebo síť elektronických komunikací, které využívá poskytovatel digitálních služeb v souvislosti se zajišťováním digitální služby podle ZKB, povinnost zavést a provádět vhodná a přiměřená bezpečnostní opatření k řízení bezpečnostních rizik. Mimo jiné poskytovateli digitálních služeb toto prováděcí nařízení Komise v čl. 2 ukládá, aby v rámci řízení bezpečnosti informací provedl analýzu rizik a řídil dodavatele. Z praktického pohledu by tedy i poskytovatelé digitální služby měli vydané varování vzít v úvahu při provádění analýzy rizik i při řízení dodavatelů, a to na základě povinností, které jim stanovuje výše zmíněné prováděcí nařízení Komise. Na informační systémy nebo sítě elektronických komunikací, které poskytovatel digitálních služeb nevyužívá v souvislosti se zajišťováním digitální služby podle ZKB, se výše uvedená povinnost nevztahuje.

3.3 Orgány nebo osoby, které nespadají pod ZKB

Orgánům a osobám, kterým ZKB neukládá povinnost zavést a provádět bezpečnostní opatření, stejně tak jako široké veřejnosti, nezakládá varování žádnou povinnost, a to ani zprostředkovaně. Je tedy na jejich zvážení, jak budou s hrozbou, na kterou varování upozorňuje, dále pracovat.

4 Řízení rizik u orgánů a osob podle ZKB a zohlednění varování

4.1 Řízení rizik

Riziko lze obecně definovat jako možnost či pravděpodobnost, že určitá hrozba využije zranitelnosti aktiva a způsobí škodu. Řízení rizik je činnost zahrnující hodnocení rizik, výběr a zavedení opatření ke zvládání rizik, sdílení informací o riziku a sledování a přezkoumání rizik. Nejdříve je stanoven rozsah aktiv, kterých se řízení bezpečnosti informací týká. Důležitost těchto aktiv je ohodnocena s ohledem na dopad při narušení bezpečnosti informací u jednotlivých aktiv, následně dojde k identifikaci a zhodnocení hrozeb a zranitelností. Tato hodnocení vedou k určení rizik a jejich řízení. Výsledná míra rizika následně indikuje požadavky na ochranu, tedy na konkrétní bezpečnostní opatření, která je nutné zavést, a tím snížit míru rizika naplnění hrozby. Účelem bezpečnostních opatření podle VKB je zajistit kybernetickou bezpečnost prostřednictvím řízení rizik, technických a organizačních opatření a schopností reagovat na incidenty.

4.2 Zohlednění varování v procesu řízení rizik

Vydané varování povinné orgány a osoby zohlední v souladu s požadavkem § 5 odst. 1 písm. h) bodu 3 VKB v rámci procesu řízení rizik.

Ze skutečností uvedených ve vydaném varování vyplývá, že **hrozbu, na kterou varování upozorňuje, je v souladu s přílohou č. 2, tabulkou č. 1 VKB potřeba hodnotit jako pravděpodobnou až velmi pravděpodobnou.** V případě užití jiné stupnice hodnocení hrozby, jak umožňuje § 5 odst. 3 VKB, je nutno tuto hrozbu ohodnotit způsobem odpovídajícím příslušné úrovni podle VKB.

4.3 Zohlednění varování při řízení dodavatelů

Proces analýzy a řízení rizik je potřeba provést také v rámci výběru dodavatele a dané hodnocení, stejně jako výsledná opatření, je třeba promítnout do smluv s dodavateli. V souladu s § 4 odst. 4 ZKB jsou orgány a osoby uvedené v § 3 písm. c) až f) ZKB 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.

Takovéto zohlednění požadavků vyplývajících z bezpečnostních opatření v míře nezbytné pro splnění povinností podle ZKB **nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži.**

5 Soulad se zákonem o zadávání veřejných zakázek

K rozhodování o tom, zda je postup zadavatele souladný s pravidly obsaženými v zákoně č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „ZZVZ“), je příslušný Úřad pro ochranu hospodářské soutěže. Podle § 36 odst. 1 ZZVZ platí, že zadavatel nesmí vytvářet při stanovování zadávacích podmínek „bezdůvodné překážky hospodářské soutěže“. V případě, že oprávněná autorita (zde Úřad), která k tomuto kroku disponuje zákonným zmocněním (zde v § 22 písm. b) ZKB), vydává akt (zde varování), který může v konkrétních případech vést k omezení hospodářské soutěže, nemůže být dodržení tohoto omezení při tvorbě zadávacích podmínek považováno za vytváření bezdůvodné překážky hospodářské soutěže. Tedy hospodářskou soutěž v tomto případě lze omezit již při stanovení zadávacích podmínek a nejedná se tím o porušení ZZVZ.

Nadto ve vztahu k orgánům a osobám uvedeným v § 3 písm. c) až f) ZKB ustanovení § 4 odst. 4 ZKB stanoví, že jsou povinny zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro jejich informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury, významný informační systém nebo informační systém základní služby 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 ZKB nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži.**

6 Doporučená opatření

Pro minimalizaci rizik spočívajících ve využívání dotčených produktů poskytovaných společností DeepSeek nebo jakoukoli její předchůdkyní, nástupnickou, mateřskou, dceřinou či přidruženou společností Úřad doporučuje implementaci následujících opatření.

6.1 Doporučení pro identifikaci a odstranění produktů, aplikací a služeb společnosti DeepSeek na služebních zařízeních

- **Komunikace se zaměstnanci a dalšími relevantními osobami** – instruujte zaměstnance (a další osoby v pracovněprávním vztahu), aby nahlásili, zda na služebních zařízeních nainstalovali nebo používali produkty, aplikace nebo webové služby společnosti DeepSeek, nebo k nim přistupovali.
- **Monitoring síťového provozu a DNS dotazů** – pomocí klíčových slov a domén lze zachytit využívání webových služeb a aplikací společnosti DeepSeek v rámci sítě organizace.
- **Auditování logů z logovacích systémů organizace** – k identifikaci, zda uživatelé přistoupili k produktům, aplikacím či webovým službám společnosti DeepSeek, nebo je stáhli či nainstalovali. Nástroje sloužící pro zaznamenávání událostí by měly být nakonfigurovány tak, aby zaznamenávaly používání internetových služeb, včetně navštívených webových stránek a staženého softwaru, a uchovávaly historii instalovaného softwaru.
- **Správa bezpečnostních nástrojů** – software nebo služby sloužící k ochraně informačních a komunikačních systémů, informací a dat. Příklady bezpečnostních nástrojů:
    - **Antivirový software** – nástroje pro nepřetržitou ochranu před škodlivým kódem se běžně používají k identifikaci škodlivých souborů, ale lze je nakonfigurovat tak, aby obecněji identifikovaly specifické typy souborů, včetně aplikací společnosti DeepSeek.
    - **Správa koncových zařízení (Endpoint Management)** – software umožňující správu koncových zařízení. Lze jej nastavit pro identifikaci nainstalovaného softwaru.
    - **Správa mobilních zařízení (Mobile Device Management)** – řešení pro správu mobilních zařízení umožňující případně i zaznamenávání používání specifických webových stránek a softwaru.
- **Aplikace funkcí kybernetické bezpečnosti** – lze využít k detekci používání konkrétních produktů nebo webových služeb. Kyberbezpečnostní funkce mohou vykonávat specializované týmy nebo být součástí běžných IT rolí, zejména v menších organizacích. Tyto funkce zahrnují:
    - **Kontrolu v rámci bezpečnostního dohledového centra (SOC)** – SOC chrání systémy a zařízení a může být využit ke kontrole logů událostí nebo žádostí o změnu nastavení systému.

- **Threat Hunting** – obvykle proaktivní činnost, která může být použita k prohledání sítí, koncových bodů a datových sad za účelem identifikace použití webových služeb nebo aplikací společnosti DeepSeek.

6.1.1 Odstranění produktů společnosti DeepSeek

Mnohé z nástrojů a řešení používaných pro identifikaci použití dotčených produktů společnosti DeepSeek lze využít i pro jejich následné odstranění.

Pro odstranění produktů a aplikací společnosti DeepSeek organizace mohou využít:

- **Endpoint administrátorské účty** – účty s endpoint administrátorskými oprávněními mohou využívat vestavěné nástroje systému k odinstalaci softwaru a aplikací.
- **Bezpečnostní nástroje** – software nebo služby pro ochranu technologií, informací a dat. Příklady:
  - **Software pro správu koncových zařízení (Endpoint Management)** – umožňuje správu zařízení, a mohou disponovat možností vzdáleného odinstalování softwaru a aplikací.
  - **Software pro správu mobilních zařízení (Mobile Device Management)** – umožňuje administrátorům odinstalovat software a aplikace ze spravovaných zařízení.

6.2 Zamezení přístupu a používání

Aby se zabránilo přístupu, měly by subjekty zvážit:

- **Informování zaměstnanců** – upozornění personálu, že nesmí přistupovat k produktům, aplikacím a službám společnosti DeepSeek ani je používat, v souladu s tímto nařízením.
- **Organizační opatření** – interní směrnice, politika, pokyn či jiné opatření k nastavení vnitřní politiky organizace, které definuje zákaz přístupu k produktům, aplikacím a službám společnosti DeepSeek a případné výjimky.
- **Filtrování webového obsahu** – povolení pouze schválených typů webového obsahu a webů s dobrou reputací a blokování přístupu ke konkrétním doménám a IP adresám Deepseeku.
- **Konfigurace webových prohlížečů** – prostřednictvím proxy serverů na bránách, které blokují přístup ke specifickým kategoriím webových stránek Deepseek, typům obsahu a doménám.

Nejrelevantnější strategie pro zamezení instalace jsou:

- **Omezení oprávnění** – zabránění stažení, instalaci a využívání neschválených aplikací pomocí řízení přístupu, práv a oprávnění účtů např. na základě principu least privilege a omezení těchto oprávnění na nezbytně nutné k výkonu náplně práce.

- **Řízení aplikací (Application Control)** – zajištění, že lze instalovat a spouštět pouze schválené aplikace. U mobilních zařízení toto řízení poskytuje software pro správu mobilních aplikací (Mobile Application Management).

Verze dokumentu			
datum	**verze**	**změněno**	**popis změny**
10. července 2025	1.0	Odbor regulace	Vytvoření dokumentu