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

Spisová značka:
350 - 303/2023
Číslo jednací:
2236/2023-NÚKIB-E/350

Brno, 8. března 2023

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 v instalaci a používání aplikace TikTok na zařízeních přistupujících k informačním a komunikačním systémům kritické informační infrastruktury, informačním systémům základní služby a významným informačním systémům.

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. Na základě skutečností zjištěných při výkonu své působnosti dospěl Úřad k tomu, že instalace a používání aplikace TikTok na zařízeních přistupujících k informačním a komunikačním systémům kritické informační infrastruktury, informačním systémům základní služby a významným informačním systémům představuje hrozbu v oblasti kybernetické bezpečnosti, a proto podle § 12 odst. 1 zákona o kybernetické bezpečnosti vydává toto varování.

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

3. Kybernetická bezpečnost nespočívá pouze na posuzování technických aspektů používaných technologií, ale při výběru technických a programových prostředků používaných při zajišťování řádného fungování informačních a komunikačních systémů a jejich dodavatelů je nutné zvážit i netechnické aspekty bezpečnosti daných technologií, tedy posoudit důvěryhodnost dodavatelů a poddodavatelů (výrobců) dané technologie. Důvěryhodnost dodavatele se pak přímo promítá do důvěryhodnosti dodané technologie a určuje úroveň rizika, které je s použitím takové technologie spojeno. Důvěra v dodavatele musí být přítomna jak na úrovni konečné podoby dodávaného řešení (kvality), tak na strategické – netechnické úrovni, a spočívá i v důvěře v podnikatelské, právní a politické prostředí, ve kterém se dodavatel pohybuje a které na něj působí.

4. Úroveň důvěryhodnosti právního prostředí některých států má přímý dopad na důvěryhodnost společností, které jsou v nich usídleny a jsou takovým právním prostředím podřízeny. U států s méně důvěryhodným právním prostředím pak nelze vyloučit, že dané společnosti budou ze strany státu nuceny upřednostnit zájmy svého státu před zájmy svých zákazníků.

5. Sociální platforma TikTok vyvinutá a provozovaná čínskou společností ByteDance patří celosvětově k nejpoužívanějším ve své kategorii. TikTok zažívá velký růst na českém trhu. V současnosti zde má cca dva miliony aktivních uživatelů.

6. Společnost ByteDance je subjektem spadajícím do působnosti čínské národní legislativy. Zákon o státní bezpečnosti (国家安全法) z roku 2015 ukládá všem čínským občanům a organizacím obecnou povinnost poskytnout pomoc státním orgánům v otázkách státní bezpečnosti. Zákon o státní zpravodajské činnosti (中华人民共和国国家情报法) z roku 2017 stanoví v 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. 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. Podle čl. 6 je tento zákon aplikovatelný i vůči institucím, organizacím a jednotlivcům, kteří organizují nebo financují špionážní aktivitu proti ČLR mimo její teritorium, přičemž za špionáž mohou čínské orgány označit široké množství aktivit. To vše bez možnosti nezávislého soudního přezkumu. Zákon o obchodních společnostech (中华人民共和国公司法 2013修订) z roku 2013 umožňuje Komunistické straně Číny (dále jen „KSČ“) účinně ovlivňovat chod soukromých společností. Podle čl. 19 musí být ve společnosti ustanovena organizace KSČ za účelem výkonu aktivit KSČ ve shodě s jejími stanovami. Společnost musí pro tyto aktivity poskytnout nezbytné podmínky. Podle pravidel 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 mají výrobci technologií povinnost nahlašovat bezpečnostní zranitelnosti čínskému Ministerstvu průmyslu a IT (dále jen „MPIT“), a to nejpozději dva dny od zjištění. MPIT pak nahlašuje nález Ministerstvu státní bezpečnosti ČLR a dalším relevantním institucím. Je zakázáno zveřejňovat

tyto zranitelnosti nebo je nahlašovat zahraničním organizacím a jednotlivcům. Výše uvedené tedy vytváří obavy, že zájmy ČLR mohou být stavěny nad zájmy uživatelů technologií společností podřízených právnímu prostředí ČLR.

7. S odvoláním na výroční zprávu Bezpečnostní informační služby (dále jen „BIS“) za rok 2021 představuje ČLR rostoucí komplexní zpravodajskou hrozbu. Podle této zprávy čínské zpravodajské služby vykonávají vlivové operace ve prospěch ČLR na úkor zájmů České republiky a jejich činnost je na našem území na vysoké úrovni. Mimo to nelze podle BIS pominout ani vysokou aktivitu čínských aktérů v oblasti kybernetických útoků zaměřovaných proti České republice a dalším členům Evropské unie a Severoatlantické aliance.

8. Ze shromážděných informací vyplývá, že TikTok sbírá excesivní množství uživatelských dat. Toto činí zejména následujícími způsoby:

    - mapování zařízení, kdy aplikace zjišťují informace o jiných spuštěných a instalovaných aplikacích,
    - obsah soukromé komunikace je ukládán na servery společnosti ByteDance,
    - pravidelná kontrola lokace zařízení,
    - přístup ke kontaktům v zařízení,
    - informace o zařízení včetně Wi-Fi SSID, předešlé konfigurace Wi-Fi, sériového čísla zařízení a SIM karty, ID zařízení, IMEI zařízení, MAC adresy, telefonního čísla, výčtu všech uživatelských účtů používaných na zařízení a kompletního přístupu ke clipboardu,
    - perzistentní přístup ke kalendáři umožňující jeho čtení a změnu, nebo
    - vynucování využití nativního prohlížeče, jenž umožňuje sledovat téměř veškerou aktivitu uživatele (např. stisknutí kláves na obrazovce).

9. Množství dat a způsob, jakým jsou sbírána, může sloužit k zacílení kybernetických útoků na konkrétní osoby a tím zvýšit riziko jejich úspěchu (např. prostřednictvím spear phishingu). Současně lze tato data zneužít k vydírání zájmových osob a narušit tak bezpečnostní nebo strategické zájmy České republiky.

10. Provozovatel aplikace TikTok veřejně deklaruje, že přestože jsou data evropských uživatelů uložena na území Spojených států amerických a Singapuru, mají k nim udělen vzdálený přístup některé subjekty sídlící v Brazílii, ČLR, Malajsii, Singapuru, USA a na Filipínách.

11. V současné době probíhá ze strany Evropské komise vyšetřování, které by mělo osvětlit, zda s ohledem na rozsáhlý sběr dat, včetně osobních údajů, které aplikace TikTok provádí, není nakládání s nimi a přístup k nim v rozporu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

12. Pozměněná verze aplikace TikTok určená pro čínský trh, aplikace Douyin, disponuje funkcionalitou stažení a instalace kódu bez vědomí uživatele. To představuje riziko stažení a instalace škodlivého kódu, jež může vést ke kompromitaci zařízení a následně i regulovaného

systému, do kterého má toto zařízení přístup. Nelze vyloučit, že podobná funkcionalita může být v budoucnu součástí i mezinárodní verze aplikace TikTok.

13. Technické analýzy z otevřených zdrojů a další informace ukazují na problematické nakládání s daty uživatelů a přístup k nim ze strany zaměstnanců Bytedance v ČLR, a to navzdory opakovaným tvrzením jeho zástupců, že se tak neděje.

14. Aplikace TikTok je určena pro použití primárně na mobilních zařízeních (zejm. mobilní telefony a tablety). Mobilní zařízení 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.

15. Výše uvedené skutečnosti ve svém souhrnu vedou k důvodné obavě z možných bezpečnostních rizik plynoucích z instalace a používání aplikace TikTok na zařízeních přistupujících k informačním a komunikačním systémům kritické informační infrastruktury, informačním systémům základní služby a významným informačním systémům.

16. 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 velkého počtu uživatelů aplikace TikTok v České republice, technických specifik aplikace, která sbírá excesivní množství citlivých a velmi snadno zneužitelných informací a dat o svých uživatelích, a právního prostředí, ve kterém společnost ByteDance operuje a jímž je vázána. Současně nelze pominout skutečnost, že na problematičnost aplikace dlouhodobě upozorňují tuzemští i zahraniční partneři a mnohé členské státy a instituce Evropské unie již přijaly vůči této aplikaci preventivní opatření.

17. V závislosti na charakteru a způsobu použití konkrétního zařízení a charakteru a citlivosti informací a dat, ke kterým má zařízení přístup, Úřad doporučuje přijmout adekvátní bezpečnostní opatření k eliminaci hrozby, na kterou toto varování upozorňuje. Úřad doporučuje zakázat instalaci a používání aplikace TikTok na zařízeních, jež mají přístup do regulovaného systému (pracovní i soukromá využívaná k pracovním účelům). V případě, že orgány nebo osoby, které jsou povinny zavést bezpečnostní opatření podle zákona o kybernetické bezpečnosti, nemají tato zařízení zařazena do rozsahu řízení bezpečnosti informací v organizaci, Úřad důrazně doporučuje revizi takového rozhodnutí. Jakékoli používání aplikace TikTok na zařízeních přistupujících k regulovaným systémům nebo ovlivňujících bezpečnost regulovaných systémů by mělo být zaneseno v procesu řízení rizik a identifikovaná rizika a přijatá opatření by měla být adekvátním způsobem komunikována v rámci organizace i směrem k relevantním dodavatelům.

18. Současně Úřad doporučuje všem fyzickým osobám, jejichž data by mohla být cílem aktivit zahraničních zpravodajských služeb (tzv. zájmové osoby, tedy osoby, které jsou například ve vysokých politických, veřejných či rozhodovacích funkcích), zvážit omezení či úplný zákaz instalace a používání aplikace TikTok i na svých osobních zařízeních.

19. Široké veřejnosti Úřad doporučuje věnovat pozornost tomu, jaké přístupy aplikace TikTok požaduje, jaká data shromažďuje a jakým způsobem s nimi nakládá. Úřad obecně doporučuje instalovat a používat pouze takové aplikace, kterým jejich uživatel důvěřuje.

20. Skutečnost, že toto varování upozorňuje na existenci hrozby v oblasti kybernetické bezpečnosti pro konkrétní technologii, neznamená, že skutečnosti obsažené v odůvodnění týkající se zejména právního prostředí, ve kterém působí společnost ByteDance, nejsou relevantní i pro další technologie pocházející z téhož právního prostředí. Úřad však na základě všech shromážděných informací ve vztahu k aplikaci TikTok shledal, že tato hrozba se jeví jako pravděpodobná až velmi pravděpodobná.

21. Pravomoc Úřadu je pro vydání tohoto varování dána ustanovením § 22 písm. b) zákona o kybernetické bezpečnosti, které jej zmocňuje k vydávání opatření. Podle § 11 odst. 2 zákona o kybernetické bezpečnosti patří mezi tato opatření i varování podle § 12 zákona o kybernetické bezpečnosti. Varování vydá Úřad podle § 12 odst. 1 zákona o kybernetické bezpečnosti, dozví-li se zejména z vlastní činnosti nebo z podnětu provozovatele národního CERT anebo od orgánů, které vykonávají působnost v oblasti kybernetické bezpečnosti v zahraničí, o hrozbě v oblasti kybernetické bezpečnosti. V souladu s § 12 odst. 2 zákona o kybernetické bezpečnosti Úřad zveřejní varování na svých internetových stránkách a oznámí je orgánům a osobám uvedeným v § 3 zákona o kybernetické bezpečnosti.

22. Úkolem Úřadu je podle § 22 písm. j) zákona o kybernetické bezpečnosti zajišťovat prevenci v oblasti kybernetické bezpečnosti. Součástí této preventivní činnosti je také poskytování informací o zjištěných hrozbách v oblasti kybernetické bezpečnosti. Pokud však hrozba dosahuje takové intenzity, že informování o ní nelze pokrýt běžnými způsoby preventivní činnosti Úřadu, je v souladu s výše uvedeným Úřad nucen přistoupit k vydání varování podle § 12 zákona o kybernetické bezpečnosti.

23. Úřad upozorňuje, že orgány nebo osoby, které jsou povinny zavést bezpečnostní opatření podle zákona o kybernetické bezpečnosti, v souvislosti s řízením rizik podle § 5 odst. 1 písm. h) bod 3 vyhlášky o kybernetické bezpečnosti při hodnocení rizik a v plánu zvládání rizik zohlední opatření podle § 11 zákona o kybernetické bezpečnosti. Jedním z těchto opatření je i varování podle § 12 zákona o kybernetické bezpečnosti. Na základě výše uvedeného Úřad považuje hrozbu ve výroku tohoto varování za pravděpodobnou až velmi pravděpodobnou. Orgány a osoby, které jsou povinny zavést bezpečnostní opatření podle zákona o kybernetické bezpečnosti, jsou proto povinny tuto hrozbu hodnotit na odpovídající úrovni, tedy na úrovni Vysoká. 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.

24. Úřad dále 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.

Digitálně podepsal:
Ing. Lukáš Kintr
Národní úřad pro kybernetickou a informační bezpečnost
Dne: 08.03.2023 10:56

NÚKIB

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