Aplikace TikTok představuje bezpečnostní hrozbu

8.3.2023 - | Národní úřad pro kybernetickou a informační bezpečnost

Na základě vydaného varování musí výše zmíněné subjekty reagovat přijetím přiměřených bezpečnostních opatření. Hrozba je hodnocena na úrovni „Vysoká“, tedy jako pravděpodobná až velmi pravděpodobná.

NÚKIB doporučuje zakázat instalaci a používání aplikace TikTok na zařízeních, jež mají přístup do regulovaného systému (pracovní i soukromá zařízení využívaná k pracovním účelům) jako nejsnadnější způsob, jak co nejvíce eliminovat uvedenou hrozbu. Současně také doporučujeme široké veřejnosti zvážit použití této aplikace a zejména to, co skrze ní sdílí. U tzv. zájmových osob, tedy osob, které jsou například ve vysokých politických, veřejných či rozhodovacích funkcích, doporučujeme aplikaci 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.

„K vydání varování jsem přistoupil na základě komplexní analýzy informací o aplikaci TikTok, které jsme získali jak z veřejných zdrojů, tak od našich spojenců. Množství sbíraných dat a nakládání s nimi, v kombinaci s právním prostředím v Číně a rostoucím počtem uživatelů v České republice, nám nedává jinou možnost, než označit TikTok za bezpečnostní hrozbu,“ říká k vydanému varování ředitel NÚKIB Lukáš Kintr a dodává: „Varování nerozlišuje mezi uživateli ze státního a soukromého sektoru. Stěžejní je pro mě to, zda by ohrožení konkrétního systému mohlo mít negativní dopad na fungování České republiky a bezpečí každého z nás.“

Celé Varování naleznete na odkazu:
https://www.nukib.cz/download/uredni_deska/2023-03-08_Varovani-TikTok_final.pdf

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.

Bezpečnostní rizika spojená s aplikací TikTok NÚKIB sleduje a vyhodnocuje dlouhodobě. V minulém roce na ně již NÚKIB upozornil vybrané subjekty z okruhu adresátů ZKB a partnerů. V roce 2022 přibyla celá řada významných zjištění a analýz, které utvrdily a prohloubily podezření spojená s aplikací, což vedlo NÚKIB k vydání tohoto varování.

Z jakého důvodu varování vydáváme?

V tomto konkrétním případě NÚKIB varování vydává, protože technologie je velmi rozšířená a její rozšíření roste. Technologie sbírá řadu informací o uživateli a jeho chování i o zařízení, na kterém běží. Tato data a informace ukládá na různých lokacích a není zcela jasné, kdo k nim má přístup. Provozovatel aplikace, společnost ByteDance, zároveň funguje v čínském právním prostředí, které samo o sobě přináší rizika. Závěry učiněné ve varování jsou podloženy analýzami z veřejných zdrojů i informacemi od tuzemských i zahraničních partnerů. Ve svém důsledku pak dostupné informace vedly k tomu, že hrozba spojená s použitím této technologie na zařízeních přistupujících do důležitých systémů (kritická informační infrastruktura, významné informační systémy a informační systémy základní služby) je vysoká, tedy že její realizace je pravděpodobná až velmi pravděpodobná.

Koho se varování týká? Pro koho je platné?

Varování se týká především povinných subjektů dle ZKB. 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 konkrétní hrozby a rozšíření technologie doporučuje NÚKIB i těmto organizacím a osobám se hrozbou zabývat.

Jaké kroky je třeba podniknout v reakci na varování?

Na základě vydaného varování musí výše zmíněné povinné osoby v rámci zavedeného systému řízení bezpečnosti provést analýzu rizik, ve které zohlední hrozbu. Následně jsou tyto subjekty povinny na riziko reagovat přijetím bezpečnostních opatření, která musí být v souladu s nastavenými metrikami pro akceptovatelnost nebo mitigaci rizika a hodnotou daného rizika.

Z pohledu veřejnosti je vhodné zvážit používání technologie a zamyslet se nad tím, co skrze aplikaci sdílí. U tzv. zájmových osob, tedy osob, které jsou například ve vysokých politických, veřejných či rozhodovacích funkcích, doporučujeme aplikaci nepoužívat.

Nejsou hrozbou také další sociální platformy podobného typu?

Je pravda, že mobilní aplikace a zejména sociální média o svých uživatelích sbírají velké množství informací. Obecně je tudíž vhodné pečlivě zvážit, jaké aplikace používat, jak se na nich chovat a jaké informace na nich sdílet. Pozornost je třeba věnovat i oprávněním, přes která se jednotlivým aplikacím povoluje přístup k datům, službám a funkcím v zařízení.

V případě TikToku jsou hrozby markantnější než u většiny srovnatelně populárních aplikací. Ten totiž o svých uživatelích sbírá velké množství dat (včetně těch velmi citlivých), které bezprostředně nepotřebuje ke svému fungování. Dále je potřeba brát v potaz čínské právní prostředí, které ukládá povinnost čínským společnostem, a tudíž i provozovatelům aplikací jako je TikTok, spolupracovat a sdílet informace se státem, a to bez náležitých právních záruk.

U jiných sociálních platforem aktuálně neevidujeme kombinaci velkého množství uživatelů, excesivního sběru dat, specifik právního prostředí, ve kterém působí provozovatel aplikace, a zároveň upozornění zpravodajských služeb na vlivové operace pocházející z tohoto prostředí. To tvoří rozdíl mezi TikTokem a dalšími aplikacemi podobného typu.

Od kdy je varování platné?

Varování je platné okamžikem svého vydání, tedy vyvěšením na úřední desce NÚKIB.

Jak jsou ohroženi běžní uživatelé, pokud budou nadále používat aplikaci TikTok?

V případě, že budou uživatelé nadále využívat aplikaci TikTok, bude o nich aplikace dále sbírat velké množství dat, která nejsou relevantní pro fungování samotné aplikace, ale mohou být v budoucnu zneužita. Samotné rozhodnutí o používání je však věcí každého jednotlivce.

https://www.nukib.cz/cs/infoservis/hrozby/1941-aplikace-tiktok-predstavuje-bezpecnostni-hrozbu