Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

3583/2022-NÚKIB-E/310 • BRNO • 24. BŘEZNA 2022

KOMUNIKAČNÍ APLIKACE S END-TO-END ŠIFROVÁNÍM: SOUČASNÝ TRH NABÍZÍ ŠIROKOU ŠKÁLU MOŽNOSTÍ, LIŠÍ SE KOMFORTEM, BEZPEČNOSTÍ A DŮVĚRYHODNOSTÍ PROVOZOVATELE

Komunikátor	Provozovatel	Státní jurisdikce	End-to-end šifrování	End-to-end šifrování pro skupinové konverzace	Podpora češtiny	Nevyžaduje osobní údaje, e-mail a/nebo telefonní číslo	Zdarma	Lze nastavit, aby se zprávy po čase smazaly	Aplikace a/nebo provozovatel nespojen s bezpečnostními incidenty**	Multiplatformní (iOS, Mac, PC, Android)
Threema	Threema GmbH	Švýcarsko	✓	✓	✓	✓	✗	✗	✓	✓
Signal	Signal Technology Foundation	USA	✓	✓	✓	✗	✓	✓	✓	✓
Telegram	Telegram Messenger Inc.	Velká Británie/ UAE	—*	✓	✓	✗	✓	✓	✗	✓
WhatsApp	Meta (dříve Facebook)	USA	✓	✓	✓	✗	✓	✓	✗	✓
Messenger	Meta (dříve Facebook)	USA	—*	✗	✓	✗	✓	✓	✗	✓
Google messages	Google	USA	—*	✗	✓	✗	✓	✗	✗	✗
Apple iMessages	Apple	USA	—*	✓	✓	✗	✓	✓	✗	✗

* **U aplikací Telegram, Messenger, Google Messages a Apple iMessages se šifrování musí manuálně aktivovat a/nebo je dostupné jen ve speciálních režimech konverzace.** K ostatním má provozovatel přístup. V případě Apple iMessage je ještě třeba deaktivovat zálohy na iCloud, které se ukládají v nezašifrované podobě.

** Viz níže.

THREEMA: MAXIMÁLNÍ BEZPEČNOST A SOUKROMÍ ZA CENU NIŽŠÍHO UŽIVATELSKÉHO KOMFORTU

Šifrovaný messenger Threema staví své renomé na maximálním důrazu na bezpečnost, anonymitu, a soukromí. **V současnosti díky důvodům uvedeným níže představuje jednu z nejlépe zabezpečených komunikačních aplikací.** Kromě využití end-to-end šifrování na veškeré formy komunikace (tedy i skupinové chaty, soubory, obrázky atd.) **disponuje i možností nastavit si unikátní hesla pro přístup k jednotlivým konverzacím.** [1] Výhodu představuje rovněž i současná švýcarská jurisdikce. [2] **Nejvýznamnější výhodou oproti jiným aplikacím je však anonymita: Threema nevyžaduje žádné osobní identifikátory, jako například telefonní číslo nebo e-mailovou adresu.** [3] Uživateli je náhodně vygenerován jeho osobní ID kód, a provozovatel aplikace tak nemá žádné informace o tom, kdo se za daným kódem nachází. **Slabé stránky Threemy se nacházejí především v uživatelském komfortu.** Threema je v porovnání s konkurencí považována za méně intuitivní, má méně funkcí a má výrazně menší uživatelskou základnu (což ovšem nepředstavuje problém v případě plošného využití v rámci organizace). **Threemu lze pořídit za cenu okolo přibližně sta korun.**[4] Ačkoliv to pro některé uživatele může představovat nevýhodu, je třeba brát v potaz, že provozovatel aplikace má tak více transparentní zdroje financování. **V současnosti není evidován žádný bezpečnostní incident (zejména prolomení šifrování) jak u aplikace, tak u jejího provozovatele.**

SIGNAL: NEJPOPULÁRNĚJŠÍ ŠIFROVANÝ KOMUNIKÁTOR NABÍZÍ BEZPEČÍ I KOMFORT, ALE MÉNĚ SOUKROMÍ

Signal je v současnosti nejpopulárnější chatovací aplikací s důrazem na bezpečnost a end-to-end šifrovaní. [5] Zašifrovány jsou stejně jako u Threemy všechny formy komunikace. Hlavní výhodou Signalu jsou uživatelské funkce, jako například skupinové videohovory, které Threema neumožnuje, či možnost nastavení automatického mazání zpráv. [6] Signal má dále víc uživatelsky přívětivých funkcí jako oblíbené kontakty, možnost upravit si vzhled aplikace, posílat animované obrázky ve formátu GIF atd. Signal rovněž klade důraz na open-source přístup a nezávislé prověření, a jeho šifrovaní považováno za velmi bezpečné. **Jistým bezpečnostním nedostatkem je navázání uživatelského profilu na telefonní číslo.** [7] **Signal proto nelze užívat zcela anonymně a provozovatel má přístup k osobnímu údaji uživatele**. **Přesto je ovšem úroveň bezpečnosti a soukromí aplikace Signal velmi vysoká.** Signal je provozován neziskovou nadací Signal Foundation sídlící v USA a její provoz je financován dary jak jednotlivých uživatelů, tak větších investorů. [8] **V současnosti není evidován žádný bezpečnostní incident spojený s aplikací či jejím provozovatelem** (občasné informace o tom, že byl Signal kompromitován, byly dosud zřejmě součástí dezinformační kampaně). [9] NÚKIB vydal doporučení pro co nejbezpečnější a nejefektivnější používání aplikace Signal.

TELEGRAM: OBSTOJNÉ BEZPEČNOSTNÍ PRVKY, ALE NIŽŠÍ NEŽ U KONKURENCE A VAZBA NA RUSKO

Telegram je populární zejména v ruskojazyčném světě. Jedním z důvodů zájmu o tuto aplikaci je její renomé „bezpečnější alternativy“ k WhatsAppu, poté co WhatsApp začal navyšovat sdílení dat se svou mateřskou společností Meta. Telegram nabízí široké spektrum sociálních a uživatelsky přívětivých funkcí. Ve srovnání s aplikacemi, které upřednostňují bezpečnost a soukromí, má ale nedostatky**. Jedním z klíčových problémů je absence plošného end-to-end šifrování. Tímto typem šifrování disponuje pouze speciální typ konverzace mezi dvěma uživateli (Secret Chat).**[10] **Skupinové konverzace jsou šifrovány až na serveru.** [11] **Dalším problémem je užívání vlastního šifrování. Šifrovací protokol MTProto není natolik důvěryhodný jako široce prověřené šifry formátu AES, a byly v něm nalezeny zranitelnosti.**[12] Vytvoření profilu Telegram vyžaduje telefonní číslo uživatele. [13] Ve výsledku tak z hlediska bezpečnosti není lepší než WhatsApp, jelikož ten umožnuje i zašifrované skupinové konverzace. **V roce 2018 ruský regulátor zakázal aplikaci Telegram v zemi, ale o dva roky později byl zákaz zrušen s tím, že Telegram bude s autoritami spolupracovat na „vyšetřování extremismu“.** [14] Není jasné, jakou konkrétní podobu tato spolupráce má. Telegram vlastní a provozuje společnost Telegram Messenger Inc., která je registrována na Britských Panenských ostrovech a působí ze Spojených Arabských Emirátů (UAE). Telegram je v současnosti nezisková platforma.

WHATSAPP: NEJPOPULÁRNĚJŠÍ CHATOVACÍ APLIKACE NA SVĚTĚ MÁ VESTAVĚNÉ BEZPEČNOSTNÍ PRVKY

WhatsApp vznikl jako alternativní metoda komunikace k SMS již v roce 2009 a nabízí primárně podobný formát, ačkoliv vede komunikaci přes internet. V současnosti je WhatsApp nejpoužívanější komunikační aplikace s téměř dvěma miliardami aktivních uživatelů.[15] Jeho primární výhodou je proto obrovská rozšířenost a uživatelská základna. **WhatsApp v současnosti nabízí end-to-end šifrování, které by mělo být automaticky aktivní pro všechny formy komunikace, jež aplikace nabízí.[16]** Nabízí proto poměrně vysokou úroveň bezpečnosti mezi aplikacemi, kde bezpečnost není primární předností. Problémem může být především soukromí. WhatsApp vyžaduje založení profilu skrze telefonní číslo. **Primárním problematickým aspektem je ale vlastník provozovatele aplikace, společnost Meta (dříve Facebook).** Meta má problematickou pověst a historii incidentů narušení soukromí uživatelů (např. kauza Cambridge Analytica).[17] **WhatsApp konstantně upravuje podmínky použití směrem k většímu sdílení dat s Meta,** a ačkoliv obsah zpráv by skrze použití end-to-end šifrování měl být nečitelný, Meta má v současnosti již přístup k metadatům, které WhatsApp vytváří.[18] V tuto chvíli není transparentní, jak WhatsApp generuje své příjmy. WhatsApp byl v minulosti rovněž kompromitován spywarem Pegasus, byť tato zranitelnost je v současnosti již opravena.[19]

MESSENGER: UŽIVATELSKY PŘÍVĚTIVÝ A SPOJENÝ S NEJVĚTŠÍ SOCIÁLNÍ SÍTÍ, ALE S MINIMEM BEZPEČNOSTNÍCH PRVKŮ

Messenger je dedikovaná aplikace pro chatovací službu sociální sítě Facebook. Jako taková se opírá o obrovskou uživatelskou základnu uživatelů Facebooku a nabízí široké množství funkcí a přístup k velkému množství dodatečného obsahu. **Messenger ovšem není ze své podstaty orientován na soukromí ani bezpečnost. Ačkoliv nabízí end-to-end šifrování, musí být manuálně zapnuto formou samostatné bezpečné konverzace s uživatelem. Běžné konverzace jsou nezašifrované a provozovatel má přístup k jejich obsahu. Možnost end-to-end šifrování se navíc týká pouze konverzace mezi dvěma uživateli.[20]** End-to-end šifrování není dostupné pro skupinové chaty, ani hlasové hovory či videohovory. K registraci a používání Messengeru uživatel potřebuje facebookový profil vázaný na e-mailovou adresu.[21] **Messenger je přímo spravován společností Meta (dříve Facebook), která má problematickou minulost, v oblasti ochrany dat a bezpečnosti uživatelů.** Messenger je rovněž jako mateřská sociální síť Facebook financován cílenou reklamou, která se zobrazuje přímo v aplikaci. Další částí obchodního modelu společnosti je prodej osobních dat uživatelů. **Messenger proto není vhodný pro provozování citlivých komunikačních kanálů.** V případě nouze je potom velmi výrazně doporučeno používat možnost šifrované konverzace.

GOOGLE MESSAGES A APPLE IMESSAGES: VESTAVĚNÉ APLIKACE CHYTRÝCH TELEFONŮ UMOŽNUJÍ OMEZENOU ŠIFROVANOU KOMUNIKACI

Chytré telefony obsahují základní aplikaci pro posílání zpráv. Ačkoliv tyto aplikace jsou primárně určené pro komunikaci skrze formát SMS, v současné době umožňují i další formy komunikace, jako je instantní chatovaní a další, za použití Rich Communication Services (RCS) protokolu.[22] **Při komunikaci přes RCS nabízejí telefony jak s iOS, tak s Androidem možnost end-to-end šifrování (RCS musí být povolen v aplikaci a podporován operátorem).[23] Mohou proto sloužit v případě potřeby jako záložní forma bezpečné komunikace, ačkoliv dedikované aplikace s důrazem na soukromí nabízejí výrazně lepší služby a komfort.** Aplikace Apple nabízí ve srovnání s Google Messages širší možnosti šifrované komunikace, jako například skupinové konverzace. **V případě Apple iMessages je ovšem potřeba mít na paměti, že pro zajištění skutečně bezpečné komunikace je třeba vypnout zálohy na iCloud, jelikož se zde zprávy ukládají v nezašifrované podobě.[24]** U obou aplikací je pak třeba dbát na to, zda se skutečně jedná o komunikaci RCS či nikoliv, jelikož zprávy formátu SMS zabezpečeny nejsou. Společnost Google je rovněž známá svým obchodním modelem zaměřeným na prodej osobních dat uživatelů. Ačkoliv Apple má na tomto poli lepší pozici, iMessages byly v minulosti kompromitovány spywarem Pegasus.[25]

ZDROJE

[1] What are private chats and how can I use them?. 2022. Threema? What are private chats and how can I use them? - Threema

[2] Všechna data jsou chráněna legislativou "ustanovení o ochraně dat švýcarskou vládou" (DPA) a "nařízení o ochraně dat švýcarskou vládou" (DPO), která nabízí jednu z nejsilnějších ochran soukromí na světě.

[3] Taylor, S. 2022. Threema Review 2022: Secure Messenger with Drawbacks. Restore Privacy. Threema Review 2022: Secure Messenger with Drawbacks (restoreprivacy.com)

[4] Threema. 20220. Google Play. Threema – Aplikace na Google Play

[5] Curry, D. 2022. Signal Revenue & Usage Statistics (2022). Business of Apps. Signal Revenue & Usage Statistics (2022) - Business of Apps

[6] Group calling. 2022. Signal Support. Group Calling - Voice or Video with Screen Sharing – Signal Support

[7] Hoffman, Ch. 2021. Can You Use Signal Without Giving It Your Contacts?. How-To Geek Can You Use Signal Without Giving It Your Contacts? (howtogeek.com)

[8] Viktor, V. 2022. The Signal Business Model – How Does Signal Make Money?. Productmint. The Signal Business Model – How Does Signal Make Money? (productmint.com)

[9] O'Flaherty, K. 2022. Signal Confirms Hack Claims Are Part Of Misinformation Campaign. Forbes. Signal Confirms Hack Claims Are Part Of Misinformation Campaign (forbes.com)

[10] Hoffman, Ch. 2021. Telegram Chats Aren't End-to-End Encrypted by Default. How-To Geek. PSA: Telegram Chats Aren't End-to-End Encrypted by Default (howtogeek.com)

[11] Nesbo, E. 2021. Why Telegram Isn't as Secure as You Think It Is. Make Use of. Why Telegram Isn't as Secure as You Think It Is (makeuseof.com)

[12] Leyden, J. 2021. Multiple encryption flaws uncovered in Telegram messaging protocol. The Daily Swig. Multiple encryption flaws uncovered in Telegram messaging protocol | The Daily Swig (portswigger.net)

[13] Hayes, R. 2021. How To Use Telegram Without a Phone Number. Tech Junkie. How To Use Telegram Without a Phone Number (techjunkie.com)

[14] Griffin, A, Carroll, O. 2020. Telegram: Russia lifts ban on private messaging app after it 'agrees to help with extremism investigations'. Independent. Telegram: Russia lifts ban on private messaging app after it 'agrees to help with extremism investigations

[15] WhatsApp - Statistics & Facts. 20220. Statista. WhatsApp - Statistics & Facts | Statista

[16] Milmo, D. 2021. WhatsApp to bring in encryption for backup chats after privacy fears. The Guardian. WhatsApp to bring in encryption for backup chats after privacy fears | WhatsApp | The Guardian

[17] Cambridge Analytica and Facebook. 2021. NY Times. WhatsApp is Re-Launching its Controversial Privacy Policy Update, Will Penalize Users that Don't Accept. Social media Today. Cambridge Analytica and Facebook: The Scandal and the Fallout So Far - The New York Times (nytimes.com)

[18] Hutchinson, A.2021. WhatsApp is Re-Launching its Controversial Privacy Policy Update, Will Penalize Users that Don't Accept | Social Media Today

[19] Shagun. 2021. Explained: Is your smartphone, Whatsapp safe against Pegasus spyware? Here's how to avoid hacking. True News Scoop. Explained: Is your smartphone, Whatsapp safe against Pegasus spyware? Here's how to avoid hacking (truescoopnews.com)

[20] Lawler, R. 2022. Messenger's end-to-end encrypted chats and calls are available to everyone. The Verge. Messenger's end-to-end encrypted chats and calls are available to everyone - The Verge

[21] Můžu se zaregistrovat v Messengeru, i když nemám Facebook účet? 2022. Facebook. Můžu se zaregistrovat v Messengeru, i když nemám Facebook účet? | Centrum nápovědy pro Messenger

[22] Dove, J. 2021. What is RCS messaging? Everything you need to know about the SMS successor. Digital Trends. What Is RCS Messaging, and Exactly How Does It Work? | Digital Trends

[23] Privacy. 2022. Apple. Privacy - Features - Apple,

[24] Hoffman, Ch. 2021. Apple's iMessage Is Secure … Unless You Have iCloud Enabled. How-To Geek. Apple's iMessage Is Secure … Unless You Have iCloud Enabled (howtogeek.com)

[25]Apple's iMessage targeted by Pegasus spyware from Israeli firm NSO, says cybersecurity watchdog. 2021. Wion. Apple's iMessage targeted by Pegasus spyware from Israeli firm NSO, says cybersecurity watchdog, World News | wionews.com

PODMÍNKY VYUŽITÍ INFORMACÍ

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách www.us-cert.gov/tlp). Informace je označena příznakem, který stanoví podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
Červená **TLP: RED**	Informace nemůže být použita jinou osobou než konkrétní osobou na straně příjemce, které byla informace poskytnuta, nebudou-li výslovně stanoveny další osoby, kterým lze tuto informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit po dohodě s původcem informace.
Oranžová **TLP: AMBER**	Informace může být sdílena pouze mezi pracovníky příjemce, kteří mají need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci. Jiným osobám, než výše uvedeným, nesmí být informace poskytnuta, nebudou-li výslovně stanoveny další osoby, kterým ji lze poskytnout.
Zelená **TLP: GREEN**	Informace může být sdílená v rámci příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály. Příjemce při předání musí zajistit důvěrnost komunikace informace. Příjemce nesmí informaci poskytnout veřejně, může ji však při splnění a zajištění stejných podmínek ochrany předat dalším partnerským subjektům příjemce.
Bílá **TLP: (WHITE)**	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.