Analýza oprávnění aplikací iOS

Brno, 30.8.2021 - Mobilní aplikace potřebují ke svému fungování data. Proto vývojáři aplikací požadují různé úrovně přístupu k informacím ve vašem mobilním zařízení. Obvykle je to kvůli zlepšení funkčnosti, ale občas může postrádat řádné odůvodnění.

Vývojáři aplikací mohou požadovat nadměrný přístup k osobním údajům z různých důvodů, včetně: nedbalého vývoje kódu, přizpůsobení vašeho prostředí, ať už v aplikaci nebo napříč aplikacemi, zpeněžení, poskytování legitimních funkcí nebo pro nekalé účely (např. pro krádež dat a další prodej bez vašeho vědomí).

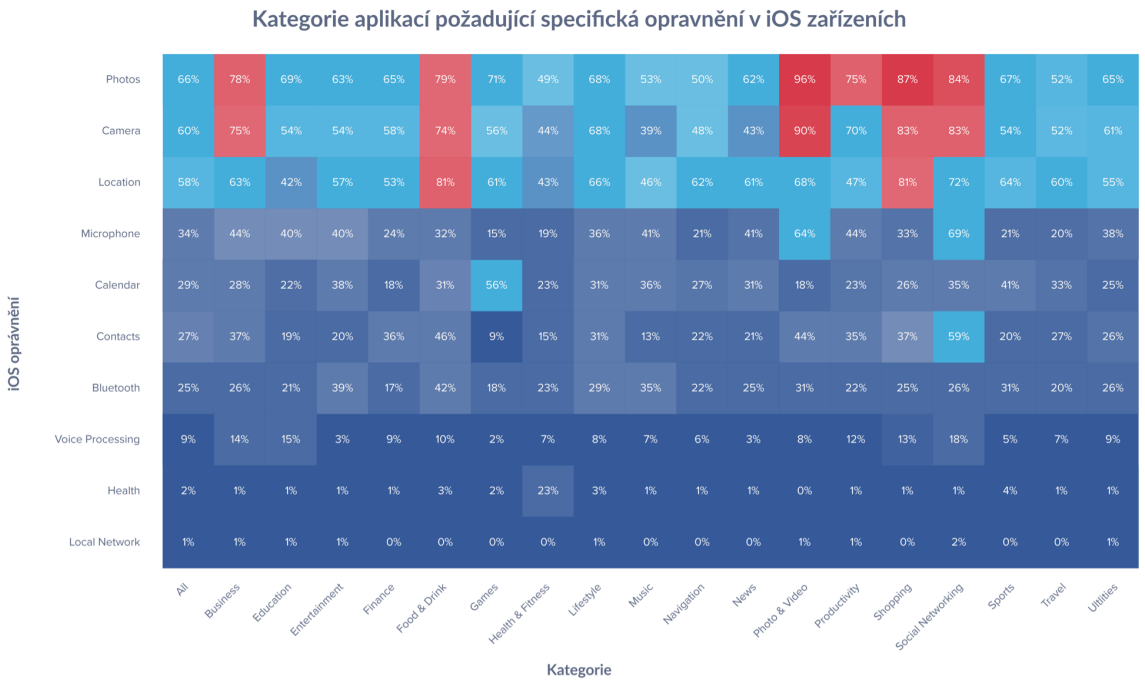
Společnosti Apple a Google - které spravují největší světové ekosystémy mobilních aplikací pro systémy iOS a Android - se snaží potírat nadměrné shromažďování údajů. Tyto dvě hlavní platformy prosazují standardy, které musí vývojáři aplikací splnit, aby získali místo v jejich obchodech s aplikacemi, a nadále zvyšují laťku, pokud jde o transparentnost oprávnění v aplikacích. Společnost Apple dokonce učinila z ochrany soukromí uživatelů téma nedávné reklamní kampaně.

Povinnost správného nakládání s daty však nemůže ležet pouze na Applu a Googlu. Vývojáři musí vyhodnotit své postupy shromažďování dat, aby minimalizovali potenciální dopad na soukromí a zároveň zachovali funkčnost svých aplikací. Na druhé straně si uživatelé musí být vědomi soukromí, kterého se vzdávají prostřednictvím sdílených informací.

Naše analýza oprávnění aplikací iOS

Abychom lépe porozuměli používání oprávnění aplikací a informacím, které se vývojáři aplikací snaží shromažďovat, prozkoumali jsme metadata ve vzorku téměř 100 000 populárních aplikací v katalogu App Store. Tento vzorek byl určen na základě aplikací, které jsou nainstalovány v rámci zákaznické základny společnosti Wandera, která spravuje 2,5 milionu zařízení. Nezahrnuli jsme miliony aplikací v App Store, které nedosáhly dostatečné množství stažení. Tato analýza byla provedena ve druhém čtvrtletí roku 2021. Metadata analyzovaná v tomto výzkumu pocházejí z agregovaných protokolů, které neobsahují osobní údaje ani údaje identifikující konkrétní společnost.

Aby byla naše analýza lépe využitelná, seskupili jsme aplikace podle jejich kategorií v App Storu.



Čtyři nejčastější vyžadovaná oprávnění

Fotografie

Z naší analýzy vyplývá, že nejčastěji požadovaným typem přístupu jsou fotografie - nejméně polovina aplikací v každé kategorii požaduje přístup k fotogalerii. Nejčastějšími kategoriemi aplikací požadujících přístup do knihovny fotografií jsou:

- Fotografie a video (96 %). Do této kategorie patří aplikace jako YouTube, FaceApp.
- Nakupování (87 %). Do této kategorie patří aplikace jako Amazon nebo eBay.
- Sociální sítě (84 %). Do této kategorie patří aplikace jako Facebook, Instagram a Twitter.

Historicky byl přístup ke knihovně fotografií buď vše, nebo nic. Pokud chtěl například uživatel nahrát snímek obrazovky na Twitter, musel Twitteru poskytnout přístup ke všem fotografiím ve své knihovně. Na tom, že aplikace sociálních médií potřebuje přístup do knihovny fotografií, není nic nekalého, ale tato úroveň přístupu je nadměrná a ve spojení se špatně vytvořenou aplikací by mohla uživatele ohrozit. Se systémem iOS 14 zavedla společnost Apple větší kontrolu oprávnění k fotografiím ze strany spotřebitelů. Nyní, když aplikace potřebuje knihovnu fotografií, musí uživateli nabídnout volbu, zda chce povolit přístup k vybraným fotografiím, nebo k celé knihovně.

Fotoaparát

Přístup k fotoaparátů je druhým nejčastěji požadovaným oprávněním. Mezi hlavní kategorie aplikací požadujících přístup k fotoaparátu patří:

- Foto a video (90 %)
- Nakupování a sociální sítě jsou na děleném druhém místě (83 %).
- Pracovní aplikace (75 %). Do této kategorie patří aplikace jako Zoom nebo Slack.

Fotoaparát je sice velmi časté oprávnění, ale velmi rizikové. S přístupem ke kameře může subjekt uživatele špehovat. To je důvod, proč organizace se speciálním bezpečnostním režimem nepovolují používání telefonů s fotoaparátem a proč někteří dodavatelé přístup k fotoaparátu zakazují nebo jej odstraňují z hardwaru.

V žalobě z roku 2020 byl Instagram obviněn ze zneužití oprávnění k fotoaparátu ke špehování uživatelů, kteří měli aplikaci otevřenou, ale s funkcí fotoaparátu neinteragovali. Instagram tvrdí, že šlo o chybu a že žádná citlivá data nebyla zneužita.

Poloha

Třetí na seznamu nejoblíbenějších požadovaných oprávnění je přístup k poloze uživatele. Mezi hlavní kategorie aplikací, které požadují informace o poloze, patří:

- Nákupy jídla a nápojů (81 %). Tato kategorie zahrnuje aplikace, jako jsou např. DoorDash, UberEats nebo Yelp.
- Sociální sítě (72 %)
- Fotografie a video (68 %)

V roce 2019 zavedly společnosti Apple i Google další úroveň volby oprávnění k určování polohy pro spotřebitele. Před systémem iOS 13 existovala dvě oprávnění k určování polohy: Při použití (na popředí) a vždy (na pozadí). Se systémem iOS 13 bylo zavedeno “povolit jednou”, které je považováno za dočasné oprávnění. Podobně před systémem Android 10 měli uživatelé k dispozici dvě možnosti: povolit nebo zakázat. První možnost znamenala, že poloha je přístupná vždy (na popředí i na pozadí) a neexistuje žádný mezistupeň, ale se systémem Android 10 bylo zavedeno třístavové povolení polohy, díky čemuž uživatelé mohli vybrat možnost "povolit pouze při používání aplikace".

Více informací o zneužití údajů o poloze najdete v tomto vyšetřování deníku The New York Times.

Mikrofon

Čtvrtým nejoblíbenějším požadavkem aplikace je přístup k mikrofonu. Mezi hlavní kategorie aplikací požadujících přístup k mikrofonu patří:

- Sociální sítě (69 %)
- Fotografie a video (64 %)
- Pracovní aplikace (produktivita) (41 %). Do této kategorie patří aplikace jako Asana, Google kalendář, TimeTree.

Stejně jako u fotoaparátu může mít přístup k mikrofonu aplikace v nesprávných rukou vážné následky. Díky možnosti aktivovat mikrofon mohou aplikace nahrávat a přenášet soukromé konverzace nebo poslouchat, co se děje kolem vás, aby tyto informace prodaly reklamním

organizacím. A v případě zneužití oprávnění by to aplikace mohly dělat bez vědomí uživatelů. V systému iOS 14 však společnost Apple zavedla oranžovou tečku, která indikuje, kdy aplikace používá mikrofon - díky tomu mohou spotřebitelé snáze zjistit, zda se neděje něco podezřelého.

Sdílení dat mezi aplikacemi

Mimo výše uvedená oprávnění dochází k velkému množství sdílení informací. Sandbox aplikací má zabránit tomu, aby aplikace mezi sebou sdílely data, ale různé postupy, jak i tak Sandbox obejít. I když spolu aplikace nekomunikují napřímo, propojením různých backendových služeb a webových interakcí si inzerent může na základě chování uživatele online spojit informace z různých zdrojů. Zde je několik příkladů sdílení informací mezi aplikacemi, které nespadají pod výše uvedená oprávnění:

Výměna informací prostřednictvím reklamních identifikátorů, které sledují a sdílejí informace o chování uživatele pro účely cílení reklamy, což si běžný uživatel pravděpodobně většinou neuvědomí. Tato výměna informací mezi aplikacemi za účelem reklamy je důvodem, proč se po vyhledání slova "sourdough" (kvásek) na Googlu ve vašem kanálu na Instagramu najednou začaly objevovat reklamy na vybavení pro pečení chleba. Nedávno získali uživatelé zařízení Apple větší kontrolu nad svým soukromím, když společnost Apple vydala v systému iOS 14.5 novou funkci “App Tracking Transparency”. Nyní se vývojáři aplikací musí ptát, zda mohou sledovat vaši aktivitu v aplikacích a na webových stránkách jiných společností.
Poznámka: naše analýza oprávnění toto oprávnění zatím nezahrnuje vzhledem k tomu že bylo vydáno teprve nedávno.

Další příklad se týká knihovny fotografií. Aplikace přistupující ke knihovně fotografií mohou mít přístup také k údajům GPS vloženým do fotografií, což umožňuje rozluštit, kde a kdy člověk byl - dokonce i kde bydlí a pracuje. Údaje o poloze se k fotografiím připojí pouze v případě, že je u fotoaparátu povolena funkce GPS. Pokud však data GPS pro fotoaparát zakážete, ztratíte některé výhody, které v rámci knihovny fotografií poskytuje. Zde je několik informací o tom, jak se vyhnout sdílení údajů o poloze fotografií při jejich odesílání.

Případ nesprávného nakládání s daty vyšel najevo v roce 2020, kdy byly společnosti LinkedIn a TikTok obviněny z kopírování obsahu ve schránce (clipboardu) uživatelů systému iOS. Problém byl objeven v beta verzi systému iOS 14, když společnost Apple přidala novou funkci ochrany soukromí, která zobrazovala rychlé vyskakovací okno, které uživatele informovalo o tom, že aplikace přečetla obsah jejich clipboardu. Na první pohled se to nemusí zdát jako důsledek, ale není neobvyklé, že lidé používají správce hesel a kopírují a vkládají přihlašovací údaje ze správce hesel na webové stránky nebo do aplikací.

Klíčové poznatky

Přestože společnosti Apple i Google zlepšily podporu ochrany osobních údajů, spotřebitelé musí sami podniknout kroky k zabezpečení svých dat. Účelem tohoto výzkumu je povzbudit uživatele, aby zvážili, které údaje sdílejí s nainstalovanými aplikacemi.

Například většina (62 %) navigačních aplikací požaduje přístup k vaší poloze. Pro umístění na mapě to dává smysl, ale proč téměř polovina z nich (48 %) požaduje také přístup k vašemu fotoaparátu? Stejně je tomu u 83 % nákupních aplikací, které požadují přístup k vašemu fotoaparátu. Pro skenování QR kódů to dává smysl, ale proč jich tolik (87 %) požaduje také přístup do vaší knihovny fotografií? Vyplatí se zamyslet se nad tím, co aplikace skutečně potřebuje ke svému fungování, než stisknete tlačítko přijmout.

Existují kategorie aplikací, které žádají o přístup více než jiné. Podle naší analýzy jsou to foto a video, nakupování a sociální sítě. Pokud máte na svém telefonu mnoho aplikací z těchto kategorií, zvažte odstranění všech, které pravidelně nepoužíváte, abyste minimalizovali riziko úniku citlivých dat.

Některá oprávnění jsou citlivější než jiná, což se u jednotlivých osob liší. Možná pracujete v oboru, kde máte v knihovně fotografií uloženy citlivé soubory. V takovém případě zvažte kontrolu každého citlivého oprávnění v rámci nastavení a zkontrolujte aplikace, které k němu mají přístup, abyste mohli odstranit ty, které by mohly představovat riziko.

Doporučení pro nastavení soukromí iPhonu

Chcete-li minimalizovat riziko, že vaše citlivé informace budou vystaveny nežádoucím stranám, doporučujeme následující kroky:

- Pečlivě si přečtěte oprávnění, když se objeví. Položte si otázku: „Potřebuje tato aplikace ke svému fungování přístup k těmto soukromým údajům?“ Pokud například aplikace pro předpověď počasí žádá o přístup k vašemu fotoaparátu nebo knihovně kontaktů, dvakrát si rozmyslete, než přístup aplikaci udělíte.
- Pravidelně kontrolujte nastavení oprávnění aplikací, abyste zjistili, k čemu mají které aplikace přístup. Na co se zaměřit: (1) aplikace, které již nepoužíváte (zvažte jejich odstranění, ale pokud nemůžete, odstraňte alespoň oprávnění k citlivým údajům); (2) aplikace, které jsou úplně nové
- Pokud jde o údaje o poloze, vždy udělujte oprávnění "pouze při používání", které je k dispozici v systémech iOS i Android.
- Odstraňte aplikace, které již nepoužíváte, abyste minimalizovali riziko výskytu chyb ve starých nebo opuštěných aplikacích. V systémech iOS i Android jsou k dispozici funkce, které umožňují nepoužívané aplikace odložit/odstranit.

Pokud dohlížíte na mobilní zařízení v rámci firmy, zvažte následující kroky:

- Přijměte bezpečnostní řešení, které nabízí prověřování aplikací. Nástroj pro prověřování aplikací může pravidelně kontrolovat aplikace na nové a vznikající zranitelnosti aplikací ve vašich mobilních zařízeních. Nástroje pro prověřování aplikací mohou také poskytnout komplexní seznam aplikací, které se používají v celém parku mobilních zařízení, doplněný o hodnocení oblíbenosti, podrobnosti o verzích a další metadata. Právě tento druh informací pomáhá IT adminům určit, jaká opatření je třeba přijmout k řešení rizikových, zastaralých nebo nekompatibilních aplikací.

- Udržujte ve svých zařízeních aktuální operační systém. Vzhledem k tomu, že společnosti Apple a Google přidávají vylepšení do nastavení oprávnění, chcete zajistit, aby je uživatelé využívali - proto používejte bezpečnostní nástroj, který dokáže označit zastaralé verze operačního systému.
- Ujistěte se, že uživatelé neprovádějí jailbreaking svých zařízení, aby si mohli instalovat aplikace třetích stran. Nejenže aplikace třetích stran představují riziko, protože nebyly prověřeny společností Apple nebo Google, ale jailbreak zařízení odstraňuje ochrany zabudované v operačním systému, takže zařízení je ve velmi rizikovém stavu.

O Wandeře

Naše řešení umožňuje firmám mít svá mobilní data pod kontrolou, zajistit bezpečnost samotných zařízení a pomocí vlastního VPN řešení zajistit také bezpečný přístup uživatelů k firemním zdrojům. Díky velkému množství rozmanitých dat, které naše platforma zpracovává, dokážeme zabránit útokům v reálném čase, a předcházet problémům, jakými jsou např. phishing nebo neplánované vysoké útraty za datový roaming. Momentálně má Wandera pobočky v Brně, Londýně a San Franciscu.

Na začátku července se stala Wandera součástí americké společnosti Jamf, která je lídrem v Apple enterprise řešení. Jamf tak rozšířil své produktové portfolio o ZTNA řešení Wandery.