

JE ČAS VYKAŠLAT SE NA GOOGLE CHROME KTERÝ SE STAL OBROVSKOU BEZPEČNOSTNÍ HROZBOU A POOHLÉDNOUT SE PO ALTERNATIVĚ

- CZ24 News | 29. března 2021



„Google se o ochranu uživatelského soukromí vůbec nestará,“ varoval tento týden server DuckDuckGo, který se na toto téma specializuje.

Tento měsíc se Google ocitl v centru nemilé pozornosti poté, co na veřejnost unikly zprávy o tom, kolik uživatelských dat Chrome sbírá. To je opravdová hrozba pro soukromé údaje. Jenže Google má na svědomí i jeden horší problém, o němž se zatím moc nepíše.

Chrome se v tomto ohledu diametrálně liší od Safari, Edge i Firefoxu a prohlášení Googlu o „prohlížeči, kde soukromí hraje prim“ zní náhle jako špatný vtíp. Popravdě řečeno je to podle mě jasný důvod, proč Chrome okamžitě přestat používat.

Když Apple loni prohlásil, že donutí vývojáře aplikací zveřejnit informace o množství shromažďovaných uživatelských dat, najednou se veškerá pozornost upřela na Google a Facebook. Leckdo usoudil, že se tyhle dva světoví datoví giganti po tomto odhalení neocitnou zrovna v nejlepším světle – a právě to se stalo.

Problém s Googlem je navíc v tom, že na rozdíl od Facebooku sedí na dvou židlích. Na jednu stranu funguje s Androidem, Gmailem, kancelářskými aplikacemi, cloudovým úložištěm a dalšími součástmi ekosystému jako ochránce soukromí, na druhou jde o reklamního obra, který na inzerci vydělává

přes sto miliard dolarů ročně a tato částka tvoří většinu jeho příjmů. V této své druhé podobě si s Facebookem nijak nezadá.

Asi málokoho tudíž překvapilo, že podle bezpečnostních štítků Applu na tom jsou tyto dva reklamní giganti úplně jinak než jejich konkurence, co se shromažďování uživatelských dat týče. Když si nějaká firma založí obchodní model na zpeněžování informací o svých uživateli, pak samozřejmě potřebuje dat co nejvíc – a Google s Facebookem v tomto ohledu rozhodně nezklamou.

„Google se o ochranu uživatelského soukromí vůbec nestará,“ varoval tento týden server DuckDuckGo, který se na toto téma specializuje. Článek reagoval na to, že právě tento týden Chrome konečně zveřejnil svůj bezpečnostní štítek. *„Jde jim jen o ochranu jejich vlastního obchodního modelu, který je na sledování uživatelů postavený. Kdyby pro ně soukromí uživatelů něco znamenalo, přestali by špehovat miliardy lidí po celém světě.“*

Autoři článku na DuckDuckGo se zaměřili na data o uživateli, která Google sbírá. Kromě toho má ovšem Google ještě podstatně větší problém – týká se jiné datové sady a je důkazem, že se Chrome výrazně liší od konkurenčních prohlížečů.

V jednom z minulých článků jsem psal, že Gmail shromažďuje více dat než jiné poštovní servery. Google v reakci upozornil na prohlášení generálního ředitele Sundara Pichaje: *„Žádné informace z aplikací, kde se primárně ukládá obsah osobního charakteru – tedy z Gmailu, Disku Google, Kalendáře nebo Fotek – nepoužíváme pro reklamní účely, tečka.“*

Možná jste si všimli, že o Chromu v tomto prohlášení nepadlo ani slovo, navíc nejde o aplikaci, kde „se primárně ukládá obsah osobního charakteru“. Na druhou stranu se v prohlížeči samozřejmě nacházejí soukromé a nesmírně citlivé informace o vyhledávání a komunikaci. A Chrome, podobně jako Gmail, se při shromažďování dat chová vskutku výjimečně hrabivě.

Se zveřejněním bezpečnostních štítků si dal Google pořádně načas, nové aktualizace vydal až nějaké tři měsíce poté, co se štítky staly povinností. Teď ovšem vidíme, jak na tom Chrome skutečně je – stejně jako jsme to přednedávnem zjistili o Gmailu.

Jak jsem tehdy psal, ochrana osobních uživatelských dat je důležitá strategie, na niž existují jen dvě odpovědi – nula, nebo jednička. A podle bezpečnostních štítků se zdá, že má Google (stejně jako Facebook) jasno a jeho prohlášení o ochraně soukromí jsou jen prázdnými frázemi.

Chrome stejně jako Gmail ukládá vaše identifikační údaje a údaje vašeho zařízení v mnoha kategoriích. Na rozdíl od Safari, Edge a Firefoxu spojuje Chrome veškerá sebraná data s konkrétními přístroji a osobami.

Safari ukládá historii navštívených stránek, data o využití prohlížeče i lokalizační informace, ale nespojuje nic z toho s uživateli. Firefox ani Edge s nimi nespojují údaje o využití prohlížeče. Ale Chrome je přiznaně ukládá všechny a všechny také propojuje s identitou uživatelů.

Není na tom nic složitého. Je holý fakt, že Chrome sbírá víc dat než kterýkoli z konkurenčních prohlížečů, ale jako jediný podle všeho neshromažďuje žádné informace, které s uživatelskými identitami propojené nejsou.

To je výmluvná a znepokojivá informace o tom, že se řídí úplně jinou strategií než konkurence. Chrome se v tomto ohledu ani nesnaží soukromí svých uživatelů jakkoli chránit. Nejde jen o konkrétní datová pole, ale o celkový přístup k osobním údajům.

„Žádná firma nevydělá několik miliard dolarů, pokud neshromáždí obrovské množství dat a pak je nezpeněží,“ komentuje to Ian Thornton-Trump, bezpečnostní ředitel společnosti Cyjax. *„Časem vždycky dojdete na křižovatku tří cest. Jedna vede ke sběru všech dat, ke kterým se dostanete, druhá k těm, která potřebujete, a na třetí jich sbíráte jen nezbytné minimum. Jenže tou třetí cestou se skoro nikdo nevydává.“*

„Proč potřebuje webový prohlížeč údaje o mých financích?“ ptá se bezpečnostní expert Sean Wright. *„Podle mě je to výmluvné dost. Vážně nevím, čím by se to dalo omluvit.“* Google patrně namítne, že se každý může rozhodnout, zda při transakci své informace poskytne. Jenže spousta lidí zvolí bezmyšlenkovitě pohodlnější cestu – a data se jen sypou.

Google poslední vývoj nijak nekomentoval, jen zdůraznil, že data potřebuje, aby mohl poskytovat slíbené služby a funkce – například upravit výsledky vyhledávání podle lokality. Jenže tady se opět projevuje rozdíl mezi funkcí a provázáním dat s konkrétními uživateli, o kterém svědčí bezpečnostní štítek.

Když Google svou práci s daty zdůvodňuje optimálním fungováním služeb, uvádí stejné argumenty jako WhatsApp. Jenže jak pak rozumět skutečnosti, že konkurenční aplikace sbírají dat mnohem méně a přitom nabízejí podobné služby a funkce?

Samozřejmě ne každý uživatel všechny informace ve všech oblastech, které jsou uvedeny na bezpečnostním štítku Googlu, skutečně poskytne – jde o nejhorší možný případ a o to, že takové informace shromažďovat lze. Proto je tak důležité praktické srovnání – údaje na bezpečnostních štítcích nelze posuzovat samostatně.

Také není zrovna fér srovnávat mainstreamové aplikace s jejich specializovanými alternativami, které si na soukromí zakládají především, tedy třeba Chrome s DuckDuckGo nebo WhatsApp se Signalem.

Ovšem Google, Apple a Microsoft porovnávat určitě lze. A srovnání e-mailových aplikací i prohlížečů všech tří gigantů pro Google nijak příznivě nevyznívá, což je dobré mít na paměti, než si do telefonu nainstalujete jeho aplikace.

Na první pohled se zdá, že se Google poučil a nějaké změny ve prospěch ochrany soukromí udělal. Nedávno jeho zástupci například prohlásili, že Google *„nebude nadále využívat nástroj IDFA (Identifier for Advertisers) v systému iOS pro personalizovanou reklamu a monitoring“*.

Kromě toho Google slíbil, že přestane používat cookies pro sledování pohybu po jednotlivých webech. Jenže podrobnější pohled odhalí, že to není tak jednoduché.

Google vydělává prodejem personalizované reklamy na základě vyhledávací historie a dalších aktivit jednotlivých uživatelů. Většina reklamy se tudíž řídí tím, co uživatel na webu hledá. A Google hodlá cookies nahradit novým systémem FLoC (Federated Learning of Cohorts), což je typicky vychytralý způsob, jak „anonymizovat“ jednotlivé uživatele jejich sdružením do skupin se shodnými znaky.

Přechod na FLoC se dočkal kritiky, protože do rukou Google soustředí příliš mnoho moci nad informacemi, které samozřejmě slouží k vydělávání peněz. Vše samozřejmě záleží na prohlížeči – a Google by tolik moci rozhodně nedostal, kdyby Chrome nad konkurencí s přehledem nevedl (momentálně má tržní podíl přes 60 procent).

„Uživatelé i ochránci soukromí musejí systém FLoC jednoznačně odmítnout,“ prohlásila organizace Electronic Frontier Foundation, *„stejně jako jiné pokusy o alternativní cesty ke sledování lidského chování na internetu. Žádáme Google, aby FLoC přestal používat a místo toho přispěl k vytváření*

uživatelsky přívětivého webového prostředí.“

Člověk často nechce, aby jeho prohlížeč analyzoval vyhledávání a sbíral uživatelská data kvůli cílené reklamě. A je logické, že prohlížeč, který údajně uživatele sleduje i v režimu inkognito, patrně nebude z těch, které na uživatelské soukromí dbají na prvním místě.

Také se nabízí otázka, zda třeba Safari nebo Edge skutečně poskytují o tolik horší služby, když data tolik neshromažďují. Nezapomeňte, že Google můžete používat i bez Chromu.

Varování před Chromem se týká především majitelů iPhonů a iPadů, kteří již nemusejí používat povinně Safari. Přejít na Chrome rozhodně není dobrý nápad. Proč si nechat shromažďovat data, když to funkčnost prohlížeče nijak nevylepší?

Pro prohlížeče platí totéž, co pro e-mailové aplikace. A než mi začnete psát, že informace o jistých datových polích vidíte i na štítcích jiných prohlížečů a e-mailových aplikací, uvědomte si, že mezi pouhým užitím dat a jejich provázaností s uživatelskou identitou je obrovský rozdíl.

Andy Yen, zakladatel a ředitel firmy ProtonMail, se ke shromažďování dat v Gmailu staví velmi kriticky. A Chrome podle něj dělá totéž: „Obrázek vydá za tisíc slov. Jediný legitimní důvod, proč by jakýkoli produkt měl sbírat data, je zabezpečení základních funkcí.

To se u jednotlivých aplikací může lišit, ale jak ukazuje tabulka, prohlížeč rozhodně ke své práci nepotřebuje všechny informace o svých uživateli, které sbírá. Největší hráči na trhu už důvěry svých zákazníků zneužívají příliš dlouho, teď je čas na alternativy.“

Z hlediska ochrany uživatelského soukromí je nejlepším prohlížečem DuckDuckGo, pro většinu uživatelů ovšem asi představuje až příliš velký krok stranou. V každém prohlížeči ovšem doporučuji přinejmenším vypnout sledování napříč navštívenými stránkami a zvážit inkognito režim, i když tím přijmete o přehled, jaké stránky jste navštívili.

DuckDuckGo tvrdí, že v současnosti zaznamenává prudký nárůst. „Podle statistik z internetových obchodů je náš prohlížeč momentálně druhý nejstahovanější ve Spojených státech, hned po Chromu,“ prohlásil zástupce firmy. Pochopitelně podporuje politiku Apple s bezpečnostními štítky v App Store: „Doufám, že se další obchody připojí.“

A tohle je jádro problému. Apple data nezpeněžuje stejným způsobem jako Google – obchodní model Apple je postavený na prodeji přístrojů a služeb v rámci vlastního ekosystému a ochrana soukromí je součástí firemní DNA od samého počátku. To se ovšem o Googlu říci nedá. Google se shromažďování dat určitě nevzdá. Zato jistě okopíruje některé aktivity Applu, aby nezůstal příliš pozadu.

V posledním desetiletí se ochraně soukromí obecně příliš nedaří. Bezplatné aplikace a platformy vydělávají pouze a jedině na uživatelských datech. Uživatelé vyměnili soukromí za pohodlí. Když ale dva největší technologičtí giganti na světě, Google a Facebook, generují většinu příjmů z reklamy a když tato reklama stojí takřka výhradně na datech uživatelů, je něco hodně špatně.

„Facebook otevřeně prohlásil, že soukromí je překonaná záležitost,“ vzpomíná bezpečnostní expert Mike Thompson slova, který Mark Zuckerberg pronesl před deseti lety, než svůj přístup k osobním údajům přece jen trochu změnil. *„Proč by si Google neměl myslet totéž? Kdyby bral Google ochranu mého soukromí vážně, neviděl bych na sociálních sítích pořád stejné reklamy.“*

Jenže o soukromí se v poslední době mluví stále víc. Máte možnost získat ho do jisté míry zpět, ale je třeba brát vážně iniciativy typu bezpečnostních štítků a zodpovědně volit aplikace podle toho, jak s daty pracují. Když si podle štítků porovnáte Chrome se Safari nebo Edge a stejně si vyberete

prohlížeč od Google, dáváte najevo, že vám shromažďování dat nevadí.

Jak už bylo řečeno, budoucnost záleží jen na nás – tedy na vás.

Zdroj: <https://www.infovojna.sk>