Výsledky Cen Velkého bratra za rok 2025
Zveřejněno 14. 4. 2026
www.bigbrotherawards.cz

Kategorie: Dlouhodobý slídil

Vítěz: Meta za dlouhodobé obelhávání veřejnosti (konkrétně s přihlédnutím ke zneužívání nástroje Meta Pixel pro sběr dat)

Společnost Meta by mohla mít v Cenách Velkého bratra stejně výsadní postavení, jako měl svého času Karel Gott ve Zlatém slavíkovi. Protože ale z našich cen nechceme učinit opakování stále téhož, tak se k udělení ceny Metě uchylujeme jen občas. A právě letos pohár trpělivosti přetekl. Cena k Metě míří za dlouhodobé obelhávání uživatelů svých služeb pokud jde o zpracování jejich údajů, které se projevilo v celé řadě kauz, za něž v minulosti už padla také řada pokut. V minulém roce pak šlo konkrétně o případ zneužívání nástroje „Meta pixel" k propojování informací z aplikací v mobilním telefonu. V reakci na odhalení měla Meta od tohoto způsobu sledování ustoupit.

Před více než 10 lety společnost Meta začala používat sledovací kód původně zvaný „Facebook pixel" a později „Meta pixel", kterému je dnes obtížné se vyhnout. Je vložený na asi pětině nejnavštěvovanějších webů. Meta pixel sbírá data o návštěvnících a předává je reklamní platformě Mety (Facebook, Instagram). Společnost skrze něj sleduje, co lidé na stránkách dělají a na základě toho jim zobrazuje reklamy nebo data jinak využívá k cílům svým nebo těch, kdo Metě zaplatí. Jde o známý princip a lidé se mu brání blokátory reklam jako je třeba uBlock Origin. Nicméně výzkumníci (viz odkaz ve zdrojích) minulý rok odhalili další způsob, jakým Meta provádí sledování, aniž by o tom uživatelé věděli.

Meta totiž našla cestu, jak na telefonech se systémem Android navázat komunikaci mezi nainstalovanými aplikacemi svých služeb a právě sledovacím „pixel" kódem. Tak společnost obešla základní bezpečnostní funkci („sandboxing") mobilních operačních systémů, která brání aplikacím komunikovat mezi sebou. Šlo o technicky důmyslné zneužití adresy localhost, díky kterému Meta vytvořila skrytý kanál mezi webovou stránkou v mobilním prohlížeči a vlastními aplikacemi.

Touto cestou Meta propojila chování konkrétních uživatelů webu s jejich identitou, pod kterou byli přihlášeni v mobilní aplikaci Facebooku nebo Instagramu. Společnost tak obcházela i opatření, která uživatelé používají pro ochranu soukromí, od používání VPN po blokování cookies.

Tento případ dle poroty je nejen jedním z mnoha případů, kdy Meta sbírala údaje způsobem, který byl v rozporu s přáním a očekáváním jejích uživatelů, které o sledování ani transparentně neinformovala. Je to důkaz hluboce zakořeněného business modelu, který stojí právě na systematickém vědomém obcházení ochranných mechanismů, kterými se uživatelé snaží získat alespoň nějakou kontrolu nad svým soukromím.

Že se společnost po všech skandálech nikterak nepoučila a hodlá v dosavadním kurzu pokračovat ukazuje i svým posledním produktem: chytrými brýlemi. Švédský server Svenska Dagbladed poukázal na masivní sběr dat z těchto brýlí, který zahrnuje intimní videa, bankovní údaje, zadávání hesel apod. Tyto data jsou pak ručně zpracovávána pro účely výuky AI modelů v centrech subdodavatele Mety společnosti Sama v keňském Nairobi.

Zdroje:

- https://www.eff.org/deeplinks/2025/06/protect-yourself-metas-latest-attack-privacy
- https://localmess.github.io/#description
- https://localmess.github.io/assets/bridges-to-self-localmess-usenix-security-26.pdf
- https://www.svd.se/a/K8nrV4/metas-ai-smart-glasses-and-data-privacy-concerns-workers-say-we-see-everything