O šifrovanie sa zaujímajú firmy, vlády, bezpečnostné služby aj právnici. Mali by ste sa aj vy

- Keď dve slová pohnú trhom
- Absolútne šifrovanie?
- Aplikácie píšu Európskej komisii
- Tento biznis sa nikdy neskončí

Malá revolúcia od Elona

Stačil jeden dvojslovný post Elona Muska a svetom sa spustila migračná vlna z WhatsAppu na iné dátové aplikácie so šifrovaním end-to-end, skrátene aj e2e.

WhatsApp totiž rozhodol, že bude nutné zdieľanie dát s Facebookom a jeho dcérskymi spoločnosťami. V oznámení zaslanom používateľom uviedol, že budú musieť súhlasiť s tým, aby Facebook a jeho dcérske spoločnosti mohli zhromažďovať údaje z WhatsAppu vrátane telefónnych čísel používateľov, telefónnych čísel kontaktov aj lokalizácie používateľov. Kto by tieto pravidlá neprijal, stratil by prístup do aplikácie.

Nové pravidlá sa netýkajú používateľov z Európskej únie, no aj tak spôsobili rozruch medzi používateľmi, ktorí húfne prechádzali na iné platformy. WhatsApp rezignoval a posunul platnosť nových podmienok až na máj. Nepomohlo.

A tak aj slovenskí používatelia objavujú čaro Signalu či Telegramu, pričom Viber sa považuje za relatívne rozšírený a používaním Threemy sa už málokto v tejto krajine chváli, aj keď profesionáli nedajú na ňu dopustiť. Dve slová dokázali celosvetovo pohnúť trhom, čo dokazuje nielen vplyv Elona Muska, ale najmä zvyšujúcu sa citlivosť používateľov na ochranu osobných údajov.

Nič nie je zadarmo, ani šifrovaná aplikácia

Po masívnom sťahovaní Signalu začali v odborných médiách novinári pátrať po jeho pôvode – a jedna z ciest vedie k investorom spojeným s bezpečnostnými agentúrami Spojených štátov. Signal vytvorila v roku 2013 už neexistujúca spoločnosť Open Whisper Systems (OWS) pod vedením „Moxie Marlinspike“, vlastným menom Matthew Rosenfeld. Vo februári 2018 prešla správa aplikácie na neziskovú organizáciu Signal Foundation, ktorá bola spustená s počiatočným kapitálom 50 miliónov amerických dolárov. Kapitál poskytol výkonný predseda nadácie, miliardár Brian Acton.

Spoločnosť OWS nikdy počas činnosti nezverejňovala finančné výkazy ani totožnosť svojich financujúcich subjektov. Rosenfeld tvrdí, že aplikácia nikdy nečerpala financovanie prostredníctvom súkromného kapitálu ani sa neusilovala o investíciu. O koľko peňazí teda išlo? Nikto netuší. Avšak je zrejmé, že najmenej 2,95 milióna amerických dolárov poskytla organizácia Open Technology Fund (OTF), na ktorej webe sa môžete dočítať, že Signal bol pôvodne vyvinutý s pomocou tohto financovania.

Organizácia OTF vznikla v roku 2012 ako pilotný program spoločnosti Radio Free Asia (RFA), ktorá je majetkom Americkej agentúry pre globálne médiá (USAGM). Agentúra USAGM je financovaná Kongresom

Spojených štátov vo výške 637 miliónov amerických dolárov ročne. Zaujímavý je vznik RFA, ktorý sa datuje do roku 1948, keď bola financovaná Ústrednou spravodajskou službou a zapojená do operácií proti komunistickým štátom.

Pri šifrovaní má slovo aj štát

Šifrovanie je dynamická téma, ktorá extrémne zaujíma aj právnikov a orgány presadzovania práva. Čoraz častejšie sa dožadujú prístupu k šifrovacím schémam, ktoré stoja za ochranou súkromia a dát používateľov mobilných zariadení. Najnovšie zistenia však naznačujú, že vlády už majú nástroje a metódy, ktoré umožňujú prístup k uzamknutým mobilom. Prístup získavajú vďaka slabým miestam v bezpečnostných schémach systémov Android a iOS.

Súčasná ochrana mobilných zariadení je postačujúca na ochranu používateľov pred potenciálnymi útokmi. Avšak odborníci dospeli k záveru, že táto ochrana v prípade špecializovaných forenzných nástrojov pre mobilné zariadenia zaostáva a trh ich ponúka, ak ide o presadzovania práva a policajných vyšetrovaní. Správa neziskovej organizácie Upturn poukazuje na príklady forenzných nástrojov pre mobilné zariadenia, ktoré použila americká polícia. V rokoch 2015 až 2019 údajne získala prístup k údajom z 50-tisíc mobilných zariadení.

Aktuálna prax to potvrdzuje, rozšírený mobilný dohľad je všadeprítomný v mnohých regiónoch sveta. Vládne agentúry po celom svete vrátane USA, Spojeného kráľovstva, Austrálie a Indie sa čoraz častejšie obracajú na technologické spoločnosti s požiadavkou na oslabenie šifrovania ich zariadení. Nezaostávajú ani štáty EÚ, ktoré čoraz hlasnejšie volajú po možnosti získania prístupu k šifrovaným dátam práve z dôvodu policajných vyšetrovaní.

Ďalšia práca pre právnikov

Európska komisia sa zatiaľ zaoberá tým, ako vyriešiť prístup k dátam v šifrovaných aplikáciách v prípade podozrenia z kriminálnych činov. Ako uviedla: „Príslušné orgány musia mať zákonnú a cielenú možnosť prístupu k údajom pri plnom rešpektovaní základných práv a príslušných zákonov o ochrane údajov a zachovaní kybernetickej bezpečnosti.“

Rada EÚ prijala v decembri 2020 uznesenie o bezpečnosti prostredníctvom šifrovania a bezpečnosti napriek šifrovaniu. V ňom zdôrazňuje podporu rozvoju, vykonávaniu a používaniu silného šifrovania ako prostriedku potrebného na ochranu základných práv a digitálnej bezpečnosti občanov, vlád, priemyslu a spoločnosti. Rovnako však dodáva, že je potrebné zabezpečiť, aby príslušné orgány presadzovania práva a justičné orgány mohli vykonávať svoje zákonné právomoci s cieľom chrániť spoločnosť a občanov.

Reakcia na uznesenie na seba nenechala dlho čakať. Iný názor majú spoločnosti, ktoré majú vo svojom portfóliu aplikácie s e2e šifrovaním. Aplikácie, respektíve ich vývojári, ProtonMail, Threema, Tresorit a Tutanota vydali spoločné vyhlásenie varujúce pred nedávnymi krokmi inštitúcií EÚ, ktoré sa snažia nájsť zadné vrátka, ako sa dostať k šifrovanej komunikácii. Poukazujú na fakt, že šifrovanie buď je, alebo nie je nasadené. Buď požívame „šifrovanie absolútne“, a teda máme aj súkromie. Alebo ho používame „so zadnými vrátkami“ a strácame tým súkromie. Poskytovať informácie v boji proti kriminalite je podľa ich

vyhlásenia pochopiteľné, ale je potrebné si uvedomiť, že šifrovanie so zadnými vrátkami môže ľahko skĺznuť k porušeniu súkromia.

Nikdy sa nekončiaci biznis

Trh so šifrovacím softvérom má viacero segmentov, akými sú šifrovanie diskov, šifrovanie súborov a priečinkov, šifrovanie databáz a šifrovanie komunikácie a cloudu. Predpokladá sa, že do roku 2025 dosiahne trh so šifrovacím softvérom 14,32 miliardy amerických dolárov, pričom zložená ročná miera rastu dosiahne až 16,2 percenta. Kľúčovým faktorom, ktorý vedie k rastu trhu, je nielen rast počtu prípadov narušenia ochrany údajov, ale aj počet a objem legislatívnych predpisov.

Najrýchlejšie rastúcim segmentom trhu je šifrovanie cloudu, keďže do hybridného a zdieľaného cloudu sa uberá čoraz viacej organizácií kvôli úsporám nákladov aj flexibilite. Podľa správy Americkej asociácie informačných technológií (ITAA – Information Technology Associaton of America) podniky presunú už do roku 2020 až 83 percent pracovnej záťaže do cloudu.

Najväčší trhový podiel na globálnom trhu so šifrovacím softvérom predpovedajú analytici Severnej Amerike. Očakáva sa, že bude popredným regiónom v oblasti zavádzania a vývoja šifrovacieho softvéru. Rastúci dopyt po dodržiavaní prísnych regulačných opatrení, prítomnosť dodávateľov šifrovacieho softvéru a podpora vlády v tejto oblasti sú hlavnými rastovými faktormi počas najbližších rokov. Veľké investície do zabezpečenia citlivých údajov v súkromnom aj verejnom sektore podporia rast trhu so šifrovacím softvérom v regióne Ázie a Pacifiku.

Zdroje

https://www.rt.com/op-ed/513732-signal-messenger-us-national-security/

https://www.wired.com/story/smartphone-encryption-law-enforcement-tools/

https://www.secunet.com/en/solutions-services/securenetworks/encryption-systems/

https://www.forbes.com/sites/forbestechcouncil/2021/01/07/encryption-isnt-the-problem-its-the-solution/?sh=237d8f091e89

https://www-businessinsider-com.cdn.ampproject.org/c/s/www.businessinsider.com/whatsapp-forcing-users-to-share-personal-data-facebook-elon-musk-2021-1?amp

https://www.marketsandmarkets.com/Market-Reports/encryption-software-market-227254588.html

https://tutanota.com/blog/posts/eu-resolution-statement-protonmail-threema-tresorit-tutanota/