

# Policie chce prohledávat komunikaci přímo na zařízeních

 lipovylit.cz/wordpress/policie-chce-prohledavat-komunikaci-primo-na-zarizenich

David Z Moravy

10. srpna 2024

Policejní a soudní orgány v Evropské unii prosazují především skenování na straně klienta, tedy vyhledávání a vyhánění soukromé komunikace přímo na zařízeních, jako jsou chytré telefony, notebooky a tablety.

von Stefan Krempf

téměř každý den zvyšují Policejní a justiční orgány EU tlak v probíhajících krypto válkách a s nimi spojených diskusích o kontroverzním scénáři „going dark“, podle kterého rostoucí end-to-end šifrování chatovacích služeb jako WhatsApp, iMessage, Facebook Messenger nebo Signal Hrozí, že vyšetřovatelé budou slepí a hluchí. „Inovační centrum EU pro vnitřní bezpečnost“ nyní vyzývá k rozšířené diskusi o použití nebo zavedení postupů k obcházení šifrování. Skupina se zaměřuje především na klientské skenování (CSS), tedy vyhledávání a export soukromé komunikace přímo na uživatelská zařízení, jako jsou chytré telefony Takové techniky si zaslouží „důkladnou kontrolu“.

Inovačního centra Výzva je součástí první zprávy o šifrování, kterou Europol zveřejnil v pondělí. Kromě policejního úřadu EU je součástí centra Eurojust, EU Lisa, která je primárně odpovědná za IT systémy pro kontrolu hranic, koordinátor EU pro boj s terorismem, Společné výzkumné centrum Komise EU a jeho Generální ředitelství pro vnitřní záležitosti. .

„V posledních letech se debata mezi individuálním soukromím a kolektivní bezpečností a integritou člověka vyvinula v konstruktivnější diskusi,“ uvádí zpráva. V této oblasti však stále existují „výzvy“, které je

třeba překonat. Klíč k úspěchu spočívá „v podpoře dialogu, spolupráce a inovací, aby bylo zajištěno, že budou respektována jak individuální práva, tak potřeba zákonného dohledu“. Podle technických odborníků není trochu šifrování o nic víc možné, než být trochu těhotná.

## **Zákonodárci a soudy už reagují**

---

„Většina členských států EU má obecná právní ustanovení pro přístup k zašifrovaným informacím,“ vysvětluje Europol & Co. Některé dokonce nedávno provedly změny stávajících vnitrostátních zákonů v oblastech „relevantních pro obcházení šifrování“. Tyto dodatky potenciálně nabízejí další příležitosti ke shromažďování a používání šifrovaných dat. Pokročilé možnosti vyhledávání a prostředky cíleného zákonného přístupu by mohly být užitečné při shromažďování šifrovaných dat.

nedávno přijatou dokumentaci EU Odborníci na vnitřní bezpečnost chválí o elektronických důkazech (e-důkazech) jako „krok správným směrem pro přístup k digitálním informacím při přeshraničním vyšetřování trestných činů“, například s ohledem na cloud. Přestože příslušné nařízení neukládá poskytovatelům služeb povinnost poskytovat údaje v prostém textu, očekávané rychlejší doručení požadovaných informací by se mohlo ukázat jako přínosné vzhledem k rozdílům v době uchovávání údajů v jednotlivých zemích EU, „která je v některých případech problematicky krátká“. Evropského Zdá se, že judikatura soudního dvora týkající se infiltrovaných šifrovaných komunikačních služeb, jako je Encrochat, rovněž upřednostňuje státní zástupce.

ve sporu o plánované CSS hraje důležitou roli kontroly chatu. Řada organizací občanské společnosti, odborníků na kybernetickou bezpečnost a IT společností se však právě minulý týden zmobilizovala v petici, kterou zahájila Global Encryption Coalition s ohledem na nejnovější „kompromisní návrh“ belgického předsednictví Rady EU o kontrole chatu. Bezpečnostní a právní obavy vyjádřené odborníky

ohledně skenování na straně klienta stále přetrvávají. To neřeší problém online distribuce materiálů obsahujících sexuální zneužívání dětí. Spíše by „byla vytvořena významná bezpečnostní rizika pro všechny občany, společnosti a vlády“.

### **Nové mobilní sítě by mělo být možné monitorovat**

---

Problémy podle zprávy způsobuje také „domácí směrování“ v sítích 4G a 5G, tedy centralizace komunikačních služeb síťovými operátory. To znamená, že osoby v rámci státních hranic, které používají cizí SIM kartu, již nelze snadno odposlouchávat. To je možné pouze v případě, že zahraniční poskytovatel služby spolupracuje s tuzemským. Z technického hlediska je „vyžadován další výzkum“, aby se zde našlo řešení, které rovněž splňuje požadavky na přístup k datům pro vyšetřovatele. Mezitím by mělo být požadováno, „aby technologie zvyšující soukromí byly deaktivovány v domácím směrování“. Orgány činné v trestním řízení také potřebují právní rámec pro používání technologií odposlechu identifikace uživatelů v podobě tzv. SUPI catcherů v mobilních sítích nové generace (5 a 6G).

V posledních dnech se již vešlo ve známost, že kontroverzní skupina EU na vysoké úrovni pro přístup k datům pro účinné vymáhání práva požaduje pomocí principu „Lawful Access by Design“ , aby byl přístup k nešifrovaným komunikačním datům integrován přímo do technologie . Dříve Co. belgická policie vedla kampaň za přístup k datovým tokům v reálném čase v prostém textu od WhatsApp & Již v dubnu evropští policejní šéfové včetně Europolu varovali vlády a digitální průmysl, aby přijaly naléhavá opatření proti end-to-end šifrování.

### **Continue Reading**

---

Previous Kurská oblast: před bitvou.

Next Šándor: Obávám se, že budeme zataženi do války

