E-Bezpečí 2025, 10(2): Page 42-45. Univerzita Palackého v Olomouci. ISSN 2571-1679.
Online: https://www.e-bezpeci.cz/index.php?view=article&id=4742

CHAT CONTROL 2.0 SCHVÁLEN STÁTY EU: KONEC SOUKROMÍ, NEBO NUTNÁ OCHRANA DĚTÍ?

Kamil KOPECKÝ

Rada Evropské unie (zástupci členských států) v uplynulých dnech podpořila kontroverzní návrh nařízení, známý jako Chat Control 2.0. Jeho cílem je bojovat proti šíření dětské pornografie (CSAM), ale způsob, jakým toho chce dosáhnout, budí vášně mezi odborníky na kyberbezpečnost i ochránci soukromí. Co přesně tento návrh znamená pro běžné uživatele a jak souvisí s nedávnou výzvou europoslanců k zákazu sociálních sítí pro děti pod 16 let?

Co je Chat Control 2.0?

Pod oficiálním názvem *Nařízení o prevenci a boji proti sexuálnímu zneužívání dětí* se skrývá legislativa, která má provozovatelům online služeb (jako jsou Messenger, WhatsApp, Instagram a další) uložit povinnost aktivně vyhledávat, nahlašovat a odstraňovat nezákonný obsah zobrazující zneužívání dětí.

Ačkoliv je cíl ochrany dětí nezpochybnitelný a ušlechtilý, problém spočívá v technickém provedení. Aby bylo možné takový obsah odhalit, musí algoritmy „vidět“ do zpráv uživatelů. To je však v přímém rozporu s **koncovým šifrováním (end-to-end encryption)**, které má zaručovat, že zprávu si přečte jen odesílatel a příjemce – nikdo jiný, ani provozovatel služby, ani stát.

Jak to má fungovat: Skenování přímo v

telefonu

Aktuálně schválený kompromisní návrh zavádí mechanismus zvaný **„upload moderation“**. Protože šifrovanou zprávu nelze přečíst během přenosu, kontrola by probíhala přímo ve vašem zařízení (tzv. *client-side scanning*) těsně předtím, než se zpráva zašifruje a odešle.

Pokud by umělá inteligence vyhodnotila, že fotka nebo video, které chcete poslat, je podezřelé, systém by odeslání zablokoval a mohl by informovat příslušné orgány. Kritici, včetně českých zástupců, varují, že tento systém fakticky zavádí „štěnici“ do kapsy každého občana a otevírá dveře plošnému sledování (mass surveillance).

Dobrovolně, nebo povinně?

Schválená verze návrhu se snaží hrany obrousit tím, že zavádí pojem „dobrovolnosti“. Služby by měly skenování zavádět dobrovolně. Hned druhým dechem však legislativa dodává, že pokud by opatření nebyla dostatečná, mohou úřady vydat tzv. **detekční příkaz**, který by skenování nařídil povinně.

Konec anonymity a ověřování věku

Chat Control 2.0 není jediným tématem, které aktuálně hýbe Bruselem. Europoslanci souběžně vyzvali k přísnější regulaci sociálních sítí, která by mohla vést k **zákazu jejich používání pro děti mladší 16 let** (případně vyžadování souhlasu rodičů).

Aby bylo možné takový zákaz vymáhat a aby fungoval Chat Control, bude nutné spolehlivě ověřit věk a identitu uživatele. To v praxi může znamenat konec anonymních účtů. Uživatelé by mohli být nuceni při zakládání účtu na WhatsAppu či Instagramu:

A. Nahrát svůj občanský průkaz.

B. Poskytnout sken obličeje (face scan).

C. Využít státní digitální identitu.

Tím by došlo k propojení online aktivit s reálnou identitou člověka, což přináší obrovská rizika v případě úniku dat.

Česká stopa: Byli jsme proti

Je důležité zmínit, že **Česká republika hlasovala proti tomuto návrhu**, stejně jako Polsko, Slovensko či Nizozemsko. Českým zástupcům vadilo především prolamování šifrování, které je považováno za základní pilíř digitální bezpečnosti (např. pro bankovnictví, komunikaci s úřady, ale i běžné soukromí). Rozhodující slovo však mělo Německo, které po dlouhém váhání návrh podpořilo, čímž zajistilo potřebnou většinu v Radě EU.

Co bude dál?

Schválení Radou EU **neznamená**, že Chat Control 2.0 začne platit zítra. Nyní začíná tzv. **trilog** – vyjednávání mezi Radou EU, Evropskou komisí a Evropským parlamentem. Právě Evropský parlament se v minulosti stavěl k prolamování šifrování velmi kriticky a preferoval cílené pátrání po podezřelých osobách před plošným skenováním všech uživatelů. Čeká nás tedy ještě tvrdý politický souboj o finální podobu textu.

Ochrana dětí vs. rizika

Z pohledu prevence je situace složitá. Na jedné straně je nutné zastavit šíření dětské pornografie a chránit děti před online predátory – a současné nástroje často nestačí. Ovšem realita je taková, že k masovému šíření pornografie dochází zcela jinými cestami, mimo sociální sítě a běžné komunikační nástroje.

Na straně druhé stojí riziko, že vytvořením „zadních vrátek“ do šifrované komunikace oslabíme bezpečnost všech dětí na internetu. Pokud existuje nástroj na skenování zpráv, může být zneužit hackery, vyděrači nebo autoritářskými režimy.

Stejně tak ale vidíme, že anonymita sociálních sítích vede k násilí, k šíření dezinformací, k masovému ovlivňování veřejného mínění (např. nedávno síť X začala na profilech zobrazovat, odkud jsou registrované účty, kde byly zaregistrovány a odkud se hlásí, a mnoho profilů, které se zdají být např. americké či evropské ve skutečnosti pochází z Indie, Afriky, Asie a jde často o tzv. trollí farmy).

Skutečná bezpečnost na internetu by neměla být volbou mezi ochranou dětí a ochranou soukromí. Efektivní řešení musí zahrnovat obojí, aniž by z každého uživatele chytrého telefonu dělalo podezřelého.

Kamil Kopecký
E-Bezpečí, Univerzita Palackého v Olomouci