Warszawa, 20 czerwca 2024 r.
KL/336/88/ET/2024

Pan
Paweł Olszewski
Sekretarz Stanu
Ministerstwo Cyfryzacji

Szanowny Panie Ministrze,

Zwracam się do Pana w imieniu Konfederacji Lewiatan, Fundacji Panoptykon oraz Związku Pracodawców Branży Internetowej IAB Polska w związku z trwającymi pracami nad projektem Rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego przepisy mające na celu zapobieganie niegodziwemu traktowaniu dzieci w celach seksualnych i jego zwalczanie oraz nowej propozycji przedstawionej przez Prezydencję Belgijską.

Zgodnie z nową propozycją Prezydencji Belgijskiej, komunikatory będą musiały wykrywać znane i nieznane przypadki CSAM oraz groomingu poprzez detekcję prowadzoną na treściach wizualnych i adresach URL (lecz nie plikach audio i wiadomościach tekstowych). Ponadto, nowa propozycja zakłada równie wykrywanie znanych przypadków CSAM za pomocą kryptograficznego i percepcyjnego hashowania obrazu oraz wykrywanie nowych, nieznanych przypadków CSAM przy użyciu sztucznej inteligencji.

Aby ograniczyć liczbę fałszywych zgłoszeń, raporty o nieznanych przypadkach CSAM mają być wykonywane dopiero po zarejestrowaniu dwóch trafień (zgodnie z mechanizmem tzw. "raportowania opóźnionego"). Przed ludzką weryfikacją wykrytego nowego materiału przeprowadzona ma być pseudonimizacja jako dodatkowy środek ochronny.

Wnioskodawcy twierdzą, że dane objęte E2EE nie wchodzą w zakres proponowanego nakazu detekcji, ponieważ odbywa się ona poprzez mechanizm

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

tzw. "upload moderation" (tj. przed zastosowaniem protokołu E2EE) i jest zależna od zgody użytkownika. Jeśli jednak użytkownik odmówi zgody, nie będzie już mógł wysyłać zdjęć, filmów ani adresów URL za pośrednictwem danego komunikatora posługującego się E2EE.

Pragniemy zaznaczyć, iż popieramy cel Komisji Europejskiej, jakim jest stworzenie kompleksowych ram prawnych zapewniających lepszą ochronę dzieci przed niegodziwym i wykorzystywaniem seksualnym. Niemniej pragniemy wyrazić poważne obawy dotyczące tych propozycji, przede wszystkim związane z:

- **Prywatnością i nadzorem:** Propozycja wymagałyby od użytkownika zainstalowania na swoim urządzeniu wraz z daną aplikacją nieprzejrzystego algorytmu, który decydowałby, czy dana treść wizualna lub link powinny być przesyłane za pośrednictwem danego komunikatora, czy też nie. Po zainstalowaniu takiej technologii na urządzeniu i wyrażeniu zgody na detekcję prowadzoną na obrazach i linkach pod kątem zgodności z bazami danych CSAM, zachodzi ryzyko zmiany przeznaczenia tej technologii w celu detekcji dowolnego innego rodzaju treści. Stwarza to ryzyko dla osób w zaufaniu posługujących się komunikatorami zaszyfrowanymi, jak np. działacze polityczni w opresyjnych reżimach czy niezależni dziennikarze, ale także dla każdego użytkownika chcącego chronić swoją prywatność. Brak wyrażenia zgody na detekcję spowoduje zaś pozbawienie możliwości wysyłania zdjęć, filmów lub linków poprzez dany komunikator, ograniczając tym samym dostęp do podstawowych funkcjonalności komunikatorów.

- **Wrażliwością ekosystemu E2EE**: Proponowane rozwiązanie otwiera drzwi do szerszych naruszeń ze strony hakerów i wrogich aktorów. Nie ma możliwości uzyskania specjalnego dostępu tylko do zdjęć i linków zawartych w wiadomościach. To wciąż oznacza budowanie „tylnych drzwi" do całego ekosystemu zaszyfrowanego komunikatora. Eksperci[1] są zgodni, że hakerzy i przestępcy mogą i znajdą sposoby, aby to wykorzystać.

[1] *Bugs in our Pockets: The Risks of Client-Side Scanning*, Hal Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Jon Callas, Whitfield Diffie, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Vanessa Teague, Carmela Troncoso, Journal of Cybersecurity, 10(1), 2024

- **Wymuszoną zgodą**: Aplikacje użytkowników zostaną bezwarunkowo zaktualizowane za pomocą omawianej technologii. W przypadku rezygnacji ze zgody na detekcję wszystkich zdjęć i linków, użytkownicy stracą możliwość udostępniania materiałów wizualnych i linków poprzez komunikator. Nawet ci użytkownicy, którzy nie wyrażą zgody na detekcję, nadal będą mieli tę funkcjonalność obecną w nowych wersjach swoich wcześniej bezpiecznych aplikacji, a więc także będą podatni na ryzyka z obszaru cyberbezpieczeństwa spowodowane wprowadzeniem do aplikacji tej nowej technologii. Ponadto, nie jest jasne, czy ten nowy rodzaj „zgody" wprowadzony w propozycji belgijskiej byłby zgodny z prawodawstwem UE i orzecznictwem TSUE.

- **Możliwościami technicznymi:** Nie jest jasne, w jaki sposób możliwe byłoby stworzenie technologii, która blokowałaby wysyłanie zdjęć i linków bez inwigilacji pozostałej korespondencji.

- **Unikaniem działania dostawców usług E2EE w jurysdykcji UE**. Próba blokowania takich dostawców spowoduje masowe wykorzystanie rozwiązań VPN, które najtaniej dostarczane są przez podmioty z krajów, które są najczęstszymi agresorami w naszej cyberprzestrzeni. Doprowadzi to do wyprowadzenia dużej ilości ruchu internetowego poza jakąkolwiek kontrolę i obniży poziom bezpieczeństwa mieszkańców EU.

- Ponadto, rozwiązanie proponowane w Rozporządzeniu nakłada na podmioty komercyjne obowiązki właściwe dla podmiotów państwowych. Nie tyko wiąże się to z wysokimi kosztami, ale przede wszystkim ceduje odpowiedzialność państwa za egzekwowanie prawa na podmioty do tego nie powołane. Jest to kapitulacja państwa, które nie tylko nie powstrzyma działań wymierzonych przeciw dzieciom, ale poniesie je do poziomu niedostępnego dla państwowych podmiotów egzekwujących prawo.

Podsumowując, biorąc pod uwagę prywatność użytkowników usług łączności elektronicznej zwracamy się do Pana o to, by Polska w trakcie prac nad projektem Rozporządzenia wyraziła sprzeciw wobec propozycji przedstawionych przez Prezydencję Belgijską.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

Deklarujemy swoją gotowość do udziału we wszystkich gremiach i procesach niezbędnych do wypracowania satysfakcjonujących rozwiązań i do przedstawienia niezbędnych informacji i analiz.

Z poważaniem

Maciej Witucki, Prezydent Konfederacji Lewiatan

Katarzyna Szymielewicz, Prezeska, Dyrektorka ds. strategii i rzecznictwa, Fundacja Panoptykon

Włodzimierz Schmidt, Prezes Zarządu, Związek Pracodawców Branży Internetowej IAB Polska

Do wiadomości:
Pan Łukasz Wojewoda – Dyrektor Departamentu Cyberbezpieczeństwa, Ministerstwo Cyfryzacji

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy