Regulacja CSAM bardziej niebezpieczna niż Pegasus

Ostatnio dużo się mówi o niebezpieczeństwach czyhających na dzieci w internecie i zapewnieniu im odpowiedniej kontroli treści. Projektowana regulacja dotycząca CSAM (Children Sexual Abuse Material) jest jednak oprotestowywana przez część środowiska i część organów europejskich. O co chodzi?

Mirosław Kutyłowski

kierownik Zakładu Kryptologii w NASK – Państwowym Instytucie Badawczym. Przez ponad 20 lat był związany z Politechniką Wrocławską, założyciel Katedry Podstaw Informatyki i badań z zakresu kryptografii na tej uczelni. Dwukrotnie członek Centralnej Komisji ds. Stopni i Tytułów, członek Komitetu Informatyki PAN. W latach 1980–2000 pracował na Uniwersytecie Wrocławskim (gdzie otrzymał wszystkie stopnie naukowe). Był stypendystą Humboldta na Uniwersytecie Technicznym w Darmstadt oraz docentem w Instytucie Heinza Nixdorfa na Uniwersytecie Paderborn. Profesor wizytujący na Uniwersytecie Xidian.

Zajmuje się głównie tematyką wrogiej kryptografii, obroną przed słabymi punktami technologii kryptograficznych oraz z rozwiązaniami implementowanymi na elektronicznych dokumentach tożsamości.

Mirosław Kutyłowski: Projektowane przepisy mają zapobiegać „niegodziwemu traktowaniu dzieci w celach seksualnych" i umożliwiać zwalczanie tego zjawiska. To rzecz niezwykle istotna, tym bardziej że prawdopodobnie nie zdajemy sobie sprawy z zasięgu i konsekwencji tego zjawiska. Wiele problemów wynika z postępu nowoczesnych technologii. Dla przykładu, słyszałem od specjalistów o istnieniu wyspecjalizowanych gangów, które trudnią się pozyskiwaniem zaufania dzieci i wmanewrowują je w sytuacje, w których stają się ofiarami szantażu. Czasami ofiary nie wytrzymują ciśnienia psychicznego i szukają ucieczki w samobójstwie.

Niestety, tego typu działalność może być prowadzona z kraju, gdzie nie sięgają europejskie organy ścigania a lokalne władze co najmniej nie współpracują z naszymi. Bariera językowa przestała stanowić jakąkolwiek barierę dla takiej przestępczej działalności. Technologie AI dają możliwość takiego wytrenowania danych w języku ofiary, że nie ma ona najmniejszych szans zorientować się w sytuacji. Ataki mogą być zautomatyzowane, masowe i autonomiczne i skuteczne. Co prawda, giganci technologiczni są wrażliwi na tego typu działania i starają się zablokować możliwości wytrenowania modeli w dyskutowanym tu kierunku, ale … to może okazać się jedynie ograniczeniem skali szkód.

Projektowana regulacja zmierza w kierunku automatycznej analizy treści przesyłanych pomiędzy użytkownikami w kierunku ochrony dzieci i adekwatnego reagowania, tak aby nie mogło dojść do niepożądanych zdarzeń.

Co w tym złego? Dlaczego na przykład Europejski Inspektor Ochrony Danych Osobowych ma tak negatywne stanowisko wobec wielu zapisów projektowanej regulacji?

Tak jak zawsze, diabeł tkwi w szczegółach. Po pierwsze, autorzy regulacji nieco optymistycznie podchodzą do możliwości technologii. Takie życzeniowe myślenie w stosunku do informatyki jest dosyć powszechne. Podobne myślenie w przypadku medycyny skutkowałoby dyrektywami czy

ustawami zobowiązującymi NFZ do opracowania skutecznego leku na nowotwory, z datą wdrożenia np. 1.01.2025 r. O ile w przypadku medycyny takich zapędów legislatorzy raczej nie mają, o tyle w branży IT i owszem.

Problem polega na tym, że z całkiem innych względów (w tym bezpieczeństwa dzieci!), komunikacja elektroniczna powinna być szyfrowana, najlepiej w trybie end-to-end, gdzie tylko odbiorca ma techniczną możliwość odzyskania zaszyfrowanej treści.

> *Postulowana regulacja zmierza więc de facto do zakazania szyfrowania w trybie end-to-end. Jej zwolennicy mówią co prawda o analizie zaszyfrowanej treści pod kątem wykrycia treści nielegalnych, ale dziś to kwestia technicznego science fiction. Science dlatego, że istnieją tzw. w pełni homomorficzne schematy szyfrowania, a fiction dlatego, że w praktyce są zupełnie nierealizowalne ze względu na koszty i nieefektywność.*

Co złego w objęciu kontrolą komunikacji i efektywnym zakazie szyfrowania end-to-end?

Wiele złego. Pegasus w porównaniu do projektowanej regulacji CSAM to problem marginalny. CSAM miałaby objąć nadzorem wszystkich mieszkańców UE. Co prawda agencje trudniące się zwalczaniem przestępczości wymierzonej w dzieci miałyby skanować dane tylko pod tym kątem, ale... bezpieczeństwo danych w UE nie powinno zależeć od bezwarunkowego zaufania do określonej instytucji czy grupy ludzi. Ponadto, jeśli zbudujemy tego typu system powszechnej inwigilacji, to tylko czekać, kiedy zostanie on wykorzystany do celów kryminalnych. Pokusa będzie zbyt wielka, a zysk znacznie większy niż ze zbudowania komputera kwantowego. Dodajmy, że włamanie się do systemu informatycznego zbudowanego przez instytucję publiczną w wyniku przetargu prowadzonego na podstawie prawa zamówień publicznych jest dużo łatwiejsze niż zbudowanie komputera kwantowego. I relatywnie wymaga minimalnego zaangażowania środków.

Autorzy propozycji CSAM nie biorą też pod uwagę innej kwestii. O ile cenzura bardzo skutecznie mogłaby gromadzić dane o zwykłych obywatelach, o tyle byłaby bezradna wobec obrotu nielegalnymi treściami przez środowiska przestępcze. Dane takie mogą być skutecznie ukryte jako kryptogramy udające losowy szum zawarty na przykład w danych graficznych. Przekazanie klucza do deszyfrowania również byłoby łatwe, tanie i niewykrywalne dla organów ścigania. Na ostatniej konferencji CRYPTO w Santa Barbara pokazywaliśmy, że wszelkie próby opanowania sytuacji przez cenzora są skazane na niepowodzenie. Tak więc obrotu nielegalnymi danymi w darknecie nie jesteśmy w stanie powstrzymać!

Wdrożenie projektowanej regulacji prowadziłoby do powstania – z pieniędzy podatnika – systemu całkowicie nieefektywnego w stosunku do docelowego zastosowania i gromadzącego bezcenne dla naszych wrogów dane. Na warsztatach w Brukseli prelegentka wykazywała skutki uboczne regulacji dla zdrowia psychicznego dzieci i prawdopodobne nadużycia wobec dzieci, co mnie, jako laika, też zastanowiło.

To co mamy robić w tej sytuacji?

Definitywnie należy zwalczać chorobę, ale nie tak, by zabiła pacjenta. Jeśli w populacji mamy do czynienia z nowotworami, to reakcją nie może być obligatoryjne usuwanie węzłów chłonnych u każdego mieszkańca UE, mimo że taką operację niekiedy onkolodzy wykonują. W medycynie nauczyliśmy się stosować procedury koncentrujące się na efektywnym leczeniu większości przypadków, przy zminimalizowanych skutkach ubocznych i w ramach realistycznych kosztów realizacji. Stosujemy te procedury, mimo że to optymalizacja w sensie globalnym, a nie w jednostkowym przypadku pacjenta. To samo musimy zrobić w przypadku problematyki związanej z CSAM.

Co konkretnie?

Osobiście jestem zwolennikiem kilku kierunków działania. Pierwszym jest zapewnienie powszechnej elektronicznej, ale zanonimizowanej weryfikacji wieku. Eliminuje to wiele zagrożeń – np. 14-latka korespondująca z osobą dorosłą lub automatem udającym osobę fizyczną od razu miałaby możliwość zorientowania się w rzeczywistej sytuacji. To nie jest panaceum na wszystkie sytuacje, ale na pewno na wiele z nich. Funkcjonalność taka przydałaby się też w innych sytuacjach: cyfryzacja obrotu wymaga znalezienia rozwiązania w zakresie weryfikacji zdolności do podejmowania czynności prawnych zgodnie np. z regułami kodeksu cywilnego. Są też przypadki zupełnie trywialne, takie jak weryfikacja wieku osób osoby kupującej piwo w kasie samoobsługowej. Nie jestem w stanie zrozumieć, dlaczego takiej funkcjonalności nie ma jeszcze np. w mObywatelu.

Jakiś inny pomysł czy technika?

Na pewno dużym problemem w świecie mediów społecznościowych (i nie tylko) jest zjawisko *Sybil attack*. Polega ono na występowaniu jednej osoby fizycznej pod wieloma pseudonimami udającymi różne osoby. W świecie niewirtualnym trudno o taki atak – bez względu na to, jak się prze-

bierzemy i ucharakteryzujemy, nie jesteśmy w stanie występować jednocześnie w kilku rolach. A świat cyfrowy to umożliwia. Czasami wymaga to pewnego wysiłku, np. kilku kart SIM, osobno dla każdej tożsamości, ale jest możliwe.

Technologie kryptograficzne mogą tu dostarczyć skutecznego rozwiązania. W skrócie chodzi o to, by za pomocą jednego klucza (np. zawartego w ulepszonym mObywatelu) móc generować odrębny pseudonim (login) dla każdego serwisu. Co więcej, tym jednym kluczem można by uwierzytelniać się wobec serwisu i nawet podpisywać dokumenty. Co istotne, za każdym razem wskazywana byłaby pseudonimowa tożsamość dla danego serwisu, a nie tożsamość rzeczywista.

A dlaczego miałoby to chronić przed tworzeniem wielu fikcyjnych tożsamości w jednym serwisie?

Przyczyna jest prosta – schemat pozwala na wygenerowanie dokładnie jednego pseudonimu dla danego serwisu. Gwarancja jest kryptograficzna, nie jest to na przykład jakiś licznik programowy.

Jest jeszcze jedna zaleta: pseudonimy są nielinkowalne. Tak więc dziecko szukające pomocy u psychiatry czy choćby u pedagoga szkolnego mogłoby automatycznie wygenerować sobie taką tożsamość do kontaktów bez obaw, że tożsamość ta zostanie skojarzona z tożsamością z elektronicznego dziennika w szkole. Dobrze zabezpieczony pseudonim również ułatwiłby ofierze nawiązanie kontaktu z organami ścigania, pokonując – dzięki anonimowości – barierę wstydu.

Brzmi to zachęcająco, ale czy taka funkcjonalność nie jest zbyt droga i trudna do wprowadzenia?

Na pewno tańsza od systemu powszechnej inwigilacji! Ale na serio, jest kilka istotnych powodów, dla których potrzebujemy takich rozwiązań. Z jednej strony chodzi o takie sprawy, jak: realne wdrożenie dyrektywy o sygnalistach, ochronę świadków w postępowaniach sądowych przy zachowaniu prawa do obrony, zeznania w sprawach trudnych dla ofiar przestępstw (w tym zwłaszcza ofiar będących dziećmi). Z drugiej strony chodzić może o uwolnienie nas od wymyślania setek loginów i haseł do różnorodnych serwisów, do których musimy się rejestrować.

To narzędzie to coś w rodzaju silnego menedżera haseł, gdzie trudno byłoby coś źle zrobić!

A jak w tym kontekście widzi Pan oprogramowanie opensource z szyfrowaniem end-to-end, np. sieć Matrix.org?

Każde rozwiązanie typu open source ma tę zaletę, że dużo więcej można sprawdzić. Produkty typu *black box*, gdzie nie mamy dostępu do „wnętrza produktu", są wymarzonym miejscem dla zaimplementowania wrogiej kryptografii. W takiej sytuacji żaden zewnętrzny audyt nie pokaże niezgodności ze specyfikacją (silne gwarancje mają źródło w zastosowanej silnej kryptografii!). Zaimplementowana zapadka daje jednocześnie możliwość deszyfrowania kryptogramów generowanych nawet wtedy, gdy klucze do szyfrowania są bezpiecznie wygenerowane przez użytkownika.

Oczywiście, oprogramowanie otwartoźródłowe też ma swoje wady. Jednym z nich mogą być rozproszone prawa autorskie i brak odpowiedzialności za całość produktu. Prawo do modyfikacji programu to nie tylko prawo do ulepszania oprogramowania, to też prawo i możliwość jego psucia!

Mamy tyle znakomitych nowych technologii i produktów kryptograficznych, jak choćby blockchain, elektroniczne dokumenty tożsamości, dobrze zabezpieczone paszporty, silne szyfrowanie komunikacji. Czy możemy czuć się w sieci bezpieczniej?

Z bezpieczeństwem w internecie jest tak, jak ze zdrowiem… „Ile cię trzeba cenić, ten tylko się dowie, kto cię stracił." Niestety, słowa Jana Kochanowskiego doskonale opisują powszechne, dosyć lekkomyślne podejście do kwestii bezpieczeństwa. O ile trudno mieć tu pretensje do „szarego internauty" (bo niby dlaczego konsument ma być specjalistą), o tyle jako społeczeństwo mamy wiele do zrobienia w skali makro.

Od zawsze uwierzytelnianie dokumentów (papierowych czy cyfrowych) bazowało na kontekście. Jeśli co miesiąc otrzymujemy rachunki za wodę, to kolejną fakturę, mającą prawidłowe dane (numer licznika i adres odbiorcy, wykazane zużycie, dane deklarowanego nadawcy), uznajemy za autentyczną i dokonujemy płatności. Podobnie reagujemy, odbierając telefon z urzędu. Dawniej prawdopodobieństwo, że przestępca włamie się do pomieszczeń biurowych i odszuka nasze dane w papierowym segregatorze, by wykorzystać je do sfabrykowania fałszywej faktury na kilkadziesiąt złotych, było znikome. Redagowanie listów wymagało dużo pracy i znajomości lokalnych realiów.

Od tamtej pory wiele się zmieniło. Przestępcy mogą wykorzystywać narzędzia sztucznej inteligencji do preparowania wiadomości, które doskonale naśladują styl językowy danej osoby, a co więcej odwołują się do właściwego kontekstu. Wystarczy, że narzędzie AI otrzyma do „trenowania" skrzynkę mailową określonej osoby, by mogło pisać w imieniu zaatakowanej osoby wiadomości. Ich adresaci nie będą w stanie zauważyć, że w istocie korespondują z automatem.

Dawniej chroniliśmy skrzynkę mailową głównie dla zachowania poufności korespondencji. Często użytkownicy robili to w sposób dosyć niedbały, tłumacząc sobie, że „przecież nie mają nic do ukrycia". Dziś każdy musi

pamiętać, że oprócz samej zawartości informacyjnej korespondencji powinniśmy chronić się przez podszyciem się pod nas przez wrogie narzędzia AI. Co więcej, chroniąc własną skrzynkę, chronimy nie tylko siebie, lecz także swoich rozmówców.

Jak się więc chronić?

„Szary internauta" ma niewielki wpływ na stosowane zabezpieczenia i może co najwyżej dołożyć własne niedbalstwo do ewentualnego niedbalstwa usługodawcy. Należy przynajmniej jednak wykorzystać wszystkie możliwości dawane przez wdrożony system tam, gdzie jest to uzasadnione ryzykiem.

Dobrym przykładem są usługi bankowe. Reagując na rosnącą skalę fraudów, Unia Europejska wprowadziła kilka lat temu obowiązek uwierzytelniania dwuskładnikowego do serwisów bankowych. Spowodowało to pewną irytację klientów zmuszanych do bardziej skomplikowanego systemu logowania i potwierdzania transakcji (nie mniejsza zapewne była frustracja dotychczasowych ofiar kradzieży tożsamości, dla których wymagania te są niewystarczające!). I jaka była reakcja? Równanie w dół wymagań uwierzytelniania, tak aby nie stracić klientów. Przykładem jest oferowanie dróg na skróty, np. możliwość określenia „zaufanych urządzeń" itp.

A co z systemami szyfrowania poczty? Może warto wskazywać na takie rozwiązania?

Warto. Każda poufna korespondencja powinna być chroniona przed dostaniem się w niepowołane ręce. Nawet gdy ufamy, że dostawca usług pocztowych nie wykorzysta dostępu do niezaszyfrowanej poczty, to co możemy wiedzieć o możliwościach adwersarza atakującego naszego dostawcę usług. Na koniec może się zdarzyć, że dostawca jest zobligowany do ujawnienia naszej korespondencji agencjom rządowym na podstawie przepisów obowiązujących w jego kraju. Szyfrując ułatwiamy więc życie naszemu dostawcy – bezpiecznie będzie mógł przekazać kryptogramy emaili, nie narażając się na kroki odwetowe ze strony Komisji Europejskiej za złamanie zasad ochrony danych osobowych. Powinniśmy wskazywać i popularyzować takie rozwiązania! Nie jest to rzecz łatwa, bo człowiek ceni sobie przede wszystkim wygodę.

Czy edukacja użytkownika wystarczy?

Oczywiście nie. Prędzej czy później zostaniemy zmuszeni do strategicznych decyzji i radykalnej zmiany podejścia w wielu obszarach. Nie będą one łatwe. Bezpieczeństwo to coś, czego nie widać i trudno za pomocą sukcesów w tej dziedzinie wygrywać wybory. Nie jest to zresztą tylko polska specyfika. W branży *security* panuje przekonanie, że łatwiej dziś zarobić na mniej lub bardziej bezwartościowych modnych produktach, niż na czymś, od czego zależy bezpieczeństwo nasze i naszych danych. Postęp dokonuje się głównie wtedy, gdy wymagania zostaną narzucone drogą prawną.

Tak, ale niekoniecznie prowadzi do postępu… Czy wprowadzenie RODO w jakikolwiek sposób poprawiło naszą sytuację? Może lepiej byłoby powstrzymać się od mnożenia przepisów?

W przypadku RODO mamy zdecydowanie do czynienia z „papierowym tygrysem", który dużo ryczy, generuje wiele kosztów, zaś w praktyce niewiele daje w zakresie ochrony danych. Z jednej strony przechodzimy przez mordęgę akceptowania *cookies* przy każdej okazji, a z drugiej – widzimy rażące praktyki łamania ochrony danych osobowych przez instytucje publiczne. Odkładając na bok problemy o charakterze w istocie kryminalnym, mamy do czynienia z błędami o charakterze strategicznym.

Każda centralizacja przetwarzania danych to w dłuższej perspektywie stworzenie problemu, dla którego nie ma dobrego rozwiązania. Każdy zbiór danych, choćby najlepiej chroniony, jest łakomym kąskiem dla naszych przeciwników czy po prostu dla świata przestępczego. Nasze możliwości i umiejętności niekoniecznie odpowiadają poziomowi i możliwościom naszych adwersarzy. Już dawno temu profesor Ross Anderson, osoba o wielkim autorytecie w branży informatycznej w Wielkiej Brytanii, wskazywał na różnicę zasobów finansowych i ludzkich między sektorem publicznym a światem przestępczym i miażdżącej przewadze tego ostatniego.

Na szczęście, w Komisji Europejskiej i w Parlamencie chyba zdano sobie sprawę z sytuacji. Regulacja eIDAS 2 idzie w kierunku rozproszenia danych związanych z identyfikacją i uwierzytelnieniem, tak aby to „podmiot danych" gromadził je i sprawował nad nimi kontrolę. W istocie jest to jedyna droga do faktycznego zapewnienia ochrony danych osobowych. Takie podejście to dla nas rewolucja, bo w Polsce informatyzacja szła w dokładnie przeciwną stronę.

Jak widać, potrzebny jest cały ekosystem narzędzi i ich kontroli. Najlepiej byłoby to zrobić razem, wspólnie w Europie, wykorzystując cały dostępny potencjał.

Rozmawiał Adam Jurkiewicz

PTI member: https://www.linkedin.com/in/adam-jurkiewicz-python--linux/
Sekcja Informatyki Szkolnej (PTI) – Member of Board: https://sis.pti.org.pl/profile/adam_jurkiewicz/
Python support for teachers: https://python.szkola.pl
Teacher · Linux · Python 3: https://github.com/abixadamj
Private Chat: @adam.jurkiewicz:matrix.org