FUNDACJA PANOPTYKON

Warszawa, 8 marca 2016 r.

UWAGI FUNDACJI PANOPTYKON[1] DO ZAŁOŻEŃ STRATEGII CYBERBEZPIECZEŃSTWA DLA RZECZYPOSPOLITEJ POLSKIEJ[2]

Fundacja Panoptykon popiera przygotowanie strategii cyberbezpieczeństwa Rzeczypospolitej – dokumentu, który uporządkuje i całościowo zaplanuje ochronę polskiej cyberprzestrzeni. Doceniamy również kształtującą się praktykę konsultowania przez Ministerstwo Cyfryzacji dokumentów o charakterze programowym, tj. strategii cyberbezpieczeństwa czy kierunków działań strategicznych Ministra Cyfryzacji w obszarze informatyzacji usług publicznych.

Zgodnie z Założeniami Strategii Cyberbezpieczeństwa dla Rzeczypospolitej Polskiej (**dalej:** Założenia) powstać ma system ostrzegania i informowania o incydentach. Jego ważnym elementem ma być system monitorowania ruchu w punktach wymiany ruchu internetowego (Internet Exchange Points, IXP). Punkty monitorowania ruchu mają powstać zarówno między operatorami krajowymi, jak i punktami wymiany z operatorami zagranicznymi. W IXP ruch ma być monitorowany pod kątem występowania anomalii, które mogą być symptomem rozległego ataku. Jak zwracają uwagę autorzy założeń, realizacja tego postulatu jest skomplikowana, bowiem pojawiać się mogą punkty wymiany realizowane *ad hoc*, np. z wykorzystaniem łącza satelitarnego. Drugim problemem jest wolumen wymienianego ruchu: prowadzenie monitorowania wymagać będzie zastosowania urządzeń o bardzo dużej mocy obliczeniowej.

Z racji na misję Fundacji Panoptykon, którą jest ochrona praw człowieka w kontekście społeczeństwa nadzorowanego, w naszym stanowisku odnosimy się jedynie do wybranego elementu Założeń – chcemy zwrócić uwagę na zagrożenia związane z planowanym stworzeniem systemu monitorowania ruchu w punktach wymiany ruchu internetowego.

Proponowane rozwiązanie należy interpretować w kontekście obowiązującego systemu prawnego. Zgodnie z ustawą z 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz. U. 2016 poz. 147), m.in. policja i Agencja Bezpieczeństwa Wewnętrznego uzyskały możliwość dostępu do danych internetowych za pośrednictwem sieci telekomunikacyjnej. Odbywać ma się to bez udziału pracowników usługodawcy świadczącego usługi drogą elektroniczną lub przy jego niezbędnym udziale. Jednakowoż dostęp ten ograniczony jest do danych **niestanowiących treści przekazu telekomunikacyjnego**. Ponadto – w naszej ocenie – niezrealizowany pozostaje wymóg sformułowany przez Trybunał Konstytucyjny w wyroku o sygn. K 23/11, zgodnie z którym ustawodawca zobowiązany został do stworzenia mechanizmu niezależnej kontroli nad udostępnianiem policji i innym służbom danych telekomunikacyjnych. Ze względu na podobny charakter danych internetowych (rozumianych w sposób wskazany w ustawie z 15 stycznia 2016 r.), postulat Trybunału jest adekwatny również do tego typu danych.

[1] Stanowisko przygotowane przez Wojciecha Klickiego.
[2] https://mc.gov.pl/aktualnosci/zaproszenie-do-konsultacji-zalozen-strategii-cyberbezpieczenstwa-dla-rp

W świetle powyższych rozważań, obawiamy się, że system monitorowania ruchu w punktach wymiany ruchu internetowego umożliwi policji i innym służbom dostęp do danych internetowych na niespotykaną dotychczas w Polsce skalę.

Problem ten ma charakter zarówno jakościowy, jak i ilościowy. Przede wszystkim dostęp do danych za pośrednictwem punktów wymiany ruchu internetowego nie będzie ograniczony do danych niestanowiących treści przekazu telekomunikacyjnego. Ponadto, może on być wykorzystywany na dużą skalę – zwłaszcza wobec planowanego zastosowania urządzeń o dużej mocy obliczeniowej.

Zwracamy uwagę, że przyjmowanie rozwiązań pozwalających na monitorowanie ruchu w punktach wymiany, było przedmiotem krytyki Parlamentu Europejskiego. W rezolucji Parlamentu Europejskiego z 12 marca 2014 r. *w sprawie realizowanych przez NSA amerykańskich programów nadzoru, organów nadzoru w różnych państwach członkowskich oraz ich wpływu na prawa podstawowe obywateli UE oraz na współpracę transatlantycką w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych*, Parlament wezwał Holandię do „powstrzymania się od rozszerzania uprawnień służb wywiadowczych w sposób umożliwiający prowadzenie nieukierunkowanego nadzoru na szeroką skalę także w odniesieniu do przewodowej komunikacji niewinnych obywateli, zwłaszcza mając na uwadze fakt, że jeden z największych punktów wymiany ruchu internetowego na świecie mieści się w Amsterdamie (AMS-IX)".

W konkluzjach rezolucji Parlament Europejski wezwał państwa członkowskie do ochrony obywateli przed nadzorem prowadzonym niezgodnie z wymogami, o których mowa w Konwencja o ochronie praw człowieka i podstawowych wolności. Dotyczy to m.in. zakazu masowej inwigilacji, w tym prowadzonej w celu zapewnienia (cyber)bezpieczeństwa narodowego. W związku z tym postulujemy przyjęcie w strategii takich rozwiązań, które wyeliminują wskazane wyżej zagrożenia.