LOKALNIE · ANALIZA

SŁUŻBY I TAK WIEDZĄ O TOBIE BARDZO DUŻO. NIE POTRZEBUJĄ DO TEGO PEGASUSA

Adam Szabelak · 15 lutego 2022

Od grudnia ub. roku polską opinię publiczną do czerwoności rozgrzewa temat inwigilacji opozycji z wykorzystaniem systemu Pegasus. W całej sprawie umyka jednak fakt, że polskie służby – nawet gdyby w ogóle nie posiadały izraelskiego oprogramowania – dysponują bardzo daleko posuniętymi uprawnieniami inwigilacyjnymi, nad którym de facto nie ma żadnej kontroli. Ciekawe jest też całe tło sprawy. Polski rząd mógł paść ofiarą „sojuszniczej" operacji wywiadowczej...

Zacznijmy jednak od początku. Zanim o Pegasusie stało się głośno, wydarzyło się kilka dość interesujących rzeczy, które mogą pomóc odpowiedzieć na pytanie – dlaczego i przez kogo temat został wyciągnięty na światło dzienne?

W listopadzie ub. roku opublikowano informację, wedle której rząd Izraela ograniczył prawie o dwie trzecie – ze 102 do 37 – liczbę krajów, którym izraelskie firmy mogą sprzedawać narzędzia inwigilacyjne i służące do cyberataków. Nowa lista odbiorców izraelskiej cyberbroni objęła tylko kraje o „sprawdzonych demokracjach", takie jak te z Europy i z Sojuszu Pięciorga Oczu. Zabrakło na niej Polski i Węgier.

W ostatnich latach oprogramowanie szpiegowskie opracowane przez izraelskie firmy takie jak Candiru i NSO Group (producent Pegasusa) zostało powiązane z łamaniem praw człowieka w dziesiątkach krajów i wykorzystywane było przez rządy do szpiegowania reporterów, aktywistów, dysydentów i rywali politycznych. Sprawa stała się szczególnie medialna po tym, jak w lipcu opublikowano wyniki dziennikarskiego śledztwa, które zostało przeprowadzone przez konsorcjum 17 redakcji, m.in. brytyjskiego *The Guardian*, francuskiego *Le Monde*, amerykańskiego *The Washington Post*. Na wspomniane izraelskie firmy Stany Zjednoczone nałożyły nawet sankcje.

Przez decyzję Izraela o odmowie obsługi i serwisowania systemów śledczych polskie służby (CBA) z chwilą wygaśnięcia zakupionych licencji straciły dostęp do Pegasusa, którego prawdopodobnie aktywnie używały od listopada 2017 roku. „Wyborcza", powołując się na swe nieoficjalne informacje, na początku grudnia podała, że „polskie służby próbowały obejść problem, usiłując kupić pokrewne oprogramowanie w USA".

„Z wizytą pojechał tam nadinsp. Jarosław Szymczyk, komendant główny policji oraz zaufany szefa MSWiA i koordynatora służb specjalnych Mariusza Kamińskiego. Oficjalnym celem podróży był udział w obchodach Dnia Pamięci Generała Pułaskiego, ale Szymczyk miał się też spotkać z przedstawicielem FBI i prosić o pomoc w kontakcie z firmami, które mogłyby sprzedać licencję na programy szpiegowskie" – czytamy w gazecie.

> **O to samo – według „GW" – zabiegał też oficer łącznikowy polskiego CBA, pracujący w USA. „Okazuje się, że plan «obejścia» Izraela jest nie do zrealizowania, bo amerykańskie spółki działają, opierając się na izraelskich rozwiązaniach i licencji, więc też muszą pytać o zgodę" – poinformowała gazeta.**

I tutaj pojawił się spory problem. Okazało się, że „sojusznicy" nie są nam dani raz na zawsze. A kupowanie od nich zaawansowanego oprogramowania inwigilacyjnego może być bardzo ryzykowne...

CZYTAJ TAKŻE: Czy prawica rozumie cyfrowego chłopa?

Pegasus a sprawa polska

Na portalu „Zaufana Trzecia Strona" w artykule, w którym uzasadniano dlaczego to prawdopodobnie CBA zakupiło Pegasusa, zamieszczono bardzo charakterystyczną opinię: „(...) inne służby, jak np. ABW, z definicji nie ufają w tym obszarze produktom pochodzenia zagranicznego. To bardzo rozsądne podejście – nigdy nie da się do końca sprawdzić, czy wykradane informacje trafiają do tego, do kogo miały trafić i w przypadku działań ABW ryzyko ujawnienia tajemnicy państwowej jest zbyt duże. Z kolei służby walczące z przestępstwami kryminalnymi nie mają takich ograniczeń".

Po oficjalnym zerwaniu komercyjnej współpracy wszystkie informacje, które mógł pozyskać producent o wykorzystaniu swojego oprogramowania, trafiły do talii kart „do wykorzystania" przeciwko polskiemu rządowi. Okazja ku temu pojawiła się bardzo szybko. 17 grudnia Sejm RP przyjął tzw. „lex TVN", ustawę od samego początku mocno krytykowaną przez USA. Kiedy czekała ona na podpis prezydenta, już 20 grudnia grupa Citizen Lab potwierdziła, że wobec kilku osób zaangażowanych społecznie lub politycznie użyto systemu Pegasus, niekoniecznie w celu walki z przestępstwami korupcyjnymi.

> **Trudno uznać to za zbieg okoliczności. Amerykanie, bardzo przecież blisko współpracujący z Izraelczykami, mogli zdecydować się na zdyscyplinowanie swojego wasala, kiedy ten zaczął przejawiać samodzielne odruchy. Grupę Citizen Lab oczywiście raczej trudno jest oskarżać o „agenturalność", jednak co najmniej dziwnym byłoby, gdyby Amerykanie nie wykorzystywali w żaden sposób tak interesującego podmiotu w swoich operacjach wpływu.**

Wykorzystanie Pegasusa przez pewne kręgi w obozie władzy do inwigilacji opozycji jest jak najbardziej możliwe. Nie należy jednak wykluczać możliwości użycia tego systemu przez podmioty zagraniczne, aby: 1) po prostu uzyskać potrzebne informacje; 2) uczynić z określonych osób „ofiary", jednocześnie przekierowując podejrzenia na rządzących, aby osłabić ich pozycję. Pamiętajmy, że Citizen Lab wskazuje tylko kto został w ten sposób zaatakowany, nie wiemy jednak nic o sprawcy. Nawet jeżeli ujawnione dane wskazują, że operował z Polski – to nie jest to wcale takie oczywiste. Profesjonaliści wiedzą, jak nadać sobie bardzo małym wysiłkiem odpowiednią tożsamość w sieci. Wciąż nie wiemy, kto tak naprawdę stał za „aferą taśmową", albo kto odpowiedzialny jest za ujawnianie „maili Dworczyka". Z dużą dozą prawdopodobieństwa stwierdzić można, że pewną rolę odegrały we wszystkich wymienionych przypadkach

podmioty zagraniczne.

Oprócz tego zarzuty o inwigilację osób niesprzyjających władzy (czy wszelkie inne wspomniane afery) trafiły na idealny grunt w postaci „polskiego piekiełka". Niestety, żyjemy w kraju, w którym racja stanu, dobro wspólne, bezpieczeństwo informacyjne – są abstrakcją. Każdy kawałek „mięsa", nawet podrzucony przez „obcych", jedna ze stron sporu politycznego zawsze podchwyci. Za każdym razem następuje później efekt kuli śnieżnej. Wystarczy, że Amerykanie/Żydzi/Niemcy/Rosjanie/ktokolwiek zainicjuje konflikt – Polacy zrobią resztę...

Służby i tak wiedzą o Tobie bardzo dużo

W całej tej dyskusji zupełnie umyka fakt, że polskie służby i tak całkiem legalnie i praktycznie bez kontroli mogą wiedzieć o nas bardzo dużo... Po kolei jednak.

Problem z nadzorem polskich służb (nie tylko specjalnych) nie jest czymś nowym. Oburzenie wciąż wzbudza sprawa „Starucha", prowokacji m.in. na Marszu Niepodległości w 2012 r. czy podpalenia budki przed rosyjską ambasadą na tymże Marszu w roku 2013. Wszystkie te sprawy zakwalifikować można jako polityczne i w każdym z ww. przypadków w związku z niejasnymi działaniami służb cierpiały niewinne osoby, a nikt nie został pociągnięty do odpowiedzialności.

> **W 2014 roku Najwyższa Izba Kontroli informowała o potrzebie stworzenia mechanizmów nadzorczych dla polskich służb. Alarmowała wtedy, że „obowiązujące przepisy ograniczają możliwość sprawowania skutecznego nadzoru nad służbami specjalnymi przez Prezesa Rady Ministrów (...), w wielu obszarach służby specjalne, pozbawione zewnętrznego cywilnego nadzoru, kontrolują same siebie".**

W tym samym roku ukazał się wyrok Trybunału Konstytucyjnego, wedle którego niektóre przepisy dotyczące uprawnień służb obowiązujące w Polsce okazały się niezgodne z Konstytucją. Ich obowiązywanie miało zakończyć się więc 18 miesięcy po publikacji wyroku w Dzienniku Ustaw RP. Jak stwierdził TK, niejawne pozyskiwanie informacji poprzez czynności operacyjno-rozpoznawcze powinno odbywać się jedynie w celu „zapobiegania poważnym przestępstwom, ich ścigania i wykrywania", a katalog przestępstw powinien być zamknięty i regularnie weryfikowany. Stwierdzono także, że nieograniczone sięganie po billingi obywateli jest niekonstytucyjne, a w większości przypadków jednostka powinna zostać także poinformowana po zakończeniu czynności o znalezieniu się w centrum zainteresowania służb, których działalność z kolei powinna być kontrolowana przez sądy.

W efekcie 15 stycznia 2016 roku przyjęto tzw. ustawę inwigilacyjną, która... de facto rozszerzyła uprawnienia inwigilacyjne polskich służb. Dlatego też została krytycznie oceniona m.in. przez Biuro Analiz Sejmowych, Krajową Radę Sądownictwa, Sąd Najwyższy czy Generalnego Inspektora Ochrony Danych Osobowych. Po przyjęciu ustawy Biuro Trybunału Konstytucyjnego stwierdziło, że „ustawa jedynie częściowo realizuje wyrok z 30 lipca 2014 r., a dodatkowo wprowadza inne rozwiązania prawne, których wyrok TK w sprawie o sygn. K 23/11 nie wymagał, bądź do których w ogóle się nie odnosił". Krytyka pozostała jednak ostatecznie bez odzewu.

Jak zauważa Fundacja Panoptykon, ustawa inwigilacyjna wprowadziła „trzy fundamentalne zmiany dotyczące uprawnień służb do pozyskiwania danych telekomunikacyjnych i internetowych".

> **Po pierwsze, ułatwiła dostęp do danych internetowych czy telekomunikacyjnych – obecnie Policja i inne służby mogą pozyskiwać te dane bezpośrednio od firm bez udziału ich pracowników z wykorzystaniem tzw. bezpiecznego łącza, przy czym brak jest jasnego określenia, czym te dane właściwie są (wiadomo tylko, że nie są treścią komunikatów).**

Mogą one dotyczyć np. długości rozmowy telefonicznej, ale nie jej przebiegu, czy adresata wysłanego maila, ale nie o jego zawartości. To ogromna wiedza, która rodzi ryzyko masowej inwigilacji i zbierania danych „na wszelki wypadek". A wiadomo, że nadużycia się zdarzają. Chociażby Policja np. sięgała po dane w kontekście wykroczeń, na co nie pozwala polskie prawo. Nie jest wiadome ile danych pozyskano bezpodstawnie i ilu osób one dotyczyły.

Po drugie, ustawa wprowadziła mechanizm pozornej kontroli nad pobieraniem danych. Sprawuje ją właściwy sąd okręgowy, a Policja lub służba specjalna w okresach półrocznych przekazują sprawozdania obejmujące liczbę przypadków pozyskania danych, ich rodzaj, a także kwalifikacje prawne czynów, w związku z którymi wystąpiono o dane. Sąd może zapoznać się z materiałami uzasadniającymi pobranie danych, ale jak wskazuje praktyka, czyni to dosyć rzadko. Powodem jest natłok spraw i brak wyspecjalizowanych w tych sprawach komórek sądowych. Jest to sytuacja całkiem odmienna od zarządzania kontroli operacyjnej (w wyniku której pozyskać można m.in. treści przekazywanych komunikatów, to właśnie tego zagadnienia dotyczy afera Pegasusa), na którą zgodę wyrazić musi sąd, a wcześniej prokurator. Podkreślić jednak trzeba, że sądy i prokuratura w przytłaczającej większości przypadków idą służbom na rękę, m.in. z wyżej wymienionych powodów. Na przykład w 2020 roku złożono wnioski dotyczące 6537 osób, a sądy odrzuciły wnioski dotyczące jedynie 35. Niewiele więcej wniosków blokowanych jest przez prokuratorów.

Po trzecie, ustawa inwigilacyjna zmniejszyła przejrzystość działania służb poprzez wprowadzenie m.in. przesłanki pozyskiwania danych w postaci „zapobiegania przestępstwom" lub „działalności analitycznej" obok pozyskiwania ich w ramach prowadzonych postępowań. Po 2016 roku zmniejszyła się także chęć służb do informowania społeczeństwa o rozmiarach prowadzonych działań, z czym wcześniej np. ABW nie miała problemu. Agencja zasłaniając się „zagrożeniem dla interesu państwa" obroniła decyzję o braku ujawniania informacji z iloma firmami internetowymi zawarła porozumienie o udostępnianiu danych internetowych.

CZYTAJ TAKŻE: Bieda, zła praca, brak mieszkań – to nasza rzeczywistość. Polska potrzebuje ludzi w czerni

Służby potrzebują skutecznego nadzoru

Polska, Łotwa i Czechy – w tych krajach UE nie ma pozasądowego ciała przyjmującego skargi obywateli na działania służb. W Polsce ponadto służby nie informują obywatela na żadnym etapie postępowania o byciu przedmiotem ich zainteresowania. Na obie te kwestie zwrócono uwagę w raporcie eksperckim „Osiodłać Pegaza", powstałym pod patronatem poprzedniego Rzecznika Praw Obywatelskich. Ich roz-

wiązanie mogłoby stworzyć szansę na uczciwsze działanie służb dysponujących jednocześnie odpowiednim kredytem zaufania społecznego. Potrzebny jest nadzór nad tym, co służby robią: jakie informacje zbierają o obywatelach, co z tymi informacjami robią, komu je przekazują. To wymóg nowoczesnego i skutecznego państwa XXI wieku.

fot: pixabay

Oryginał: https://nlad-kopia1113.instawp.site/sluzby-i-tak-wiedza-o-tobie-bardzo-duzo-nie-potrzebuja-do-tego-pegasusa/

WSPÓŁTWÓRZ NOWY ŁAD

Za Nowym Ładem stoją czytelnicy, którzy dorzucają się do jego istnienia. Dołącz do nich — jednorazowo, w kwocie, która Ci odpowiada.

DOŁĄCZAM

wspieram.nlad.pl

Zeskanuj, aby wesprzeć