Czy izraelskie narzędzie do inwigilacji byłoby bezpieczne w rękach polskich służb?

10 września 2019

W polskich mediach głośno w ostatnich tygodniach o nowym zakupie dokonanym podobno przez Centralne Biuro Antykorupcyjne – szpiegowskim programie Pegasus. Sprawę ewentualnego zakupu przez polskie służby systemu Pegasus i jego wpływem na polską scenę polityczną oraz życie zwykłych obywateli skomentował politolog dr Mateusz Piskorski.

https://www.youtube.com/watch?v=hn3wzPreuKI

– Co to takiego system inwigilacji Pegasus i czy to faktycznie groźne?

– Nie jestem informatykiem, ani tym bardziej specjalistą w zakresie szpiegostwa cyfrowego. Przeczytałem jednak sporo opinii ekspertów na ten temat, tłumaczących dość przystępnie, na czym polega problem. Otóż – w odróżnieniu od systemów masowej inwigilacji współpracujących z analizą big data i sztuczną inteligencją, które polegają m.in. na wychwytywaniu i analizowaniu słów-kluczy w komunikacji elektronicznej – Pegasus dedykowany jest śledzeniu, pełnej, totalnej inwigilacji jednostek uznanych z jakichś względów przez organy państwa za stanowiące zagrożenie. A zatem jest to system bardziej sterowany manualnie, w zależności od arbitralnego doboru obiektu zainteresowania służb, pozwalający też na określoną kreatywność ze strony jego dysponentów. Można powiedzieć, że nie jest to inwigilacja zautomatyzowana i prewencyjna, lecz inwigilacja zindywidualizowana i represyjna. Pegasus umożliwia bowiem gromadzenie wszelkich danych, a właściwie działa niczym sterowany wirus, który przejmuje pełną kontrolę nad smartfonem czy innym urządzeniem elektronicznym.

Nie tylko można w ten sposób każdego podsłuchiwać, ale można też np. wykonywać zdjęcia czy filmować zdalnie jego i jego otoczenie, odczytywać nie tylko pocztę elektroniczną, ale też wiadomości wysyłane i odbierane przez inne komunikatory, przeglądać i ingerować w pliki, nawet te znajdujące się w tzw. chmurze. Zakres pozyskiwanych w ten sposób informacji będzie na tyle duży, że ich dysponenci będą mogli wykorzystywać je w dowolny sposób, także posługując się manipulacją.

– Wcześniej też Polska słynęła z inwigilowania nie tylko swoich obywateli, ale także obywateli innych krajów znajdujących się na jej terytorium, np. zagranicznych dziennikarzy…

– Tak, tyle, że te tendencje ulegają niebezpiecznemu nasileniu, a ponadto pojawia się coraz doskonalszy sprzęt. Pegasus to dzieło izraelskiej firmy NSO Group, założonej przez byłych oficerów wywiadu wojskowego Aman, a konkretnie Jednostki 8200, zajmującej się szpiegostwem elektronicznym, znanej m.in. z wykrytego w 2010 roku wirusa – robaka Stuxnet, który posłużył do złośliwego ataku na irański sektor jądrowy. Ich oprogramowanie miało być wykorzystywane do walki z terroryzmem, jednak z czasem przedsięwzięcie uległo komercjalizacji, zainwestowali w nie m.in. przedstawiciele amerykańskich funduszy inwestycyjnych. Efekt: działanie Pegasusa odnotowano w kilkudziesięciu krajach, w tym w Polsce, już w 2018 roku. Badająca to zagrożenie grupa naukowców i ekspertów z kanadyjskiego CitizenLab przy Uniwersytecie w Toronto odnotowała pewną prawidłowość: kontrahentami NSO Group są prawdopodobnie zazwyczaj reżimy autorytarne, oskarżane o łamanie praw człowieka i obywatela. Rodzi się jednak pytanie do władz izraelskich: skoro za wszystkim stoją byli funkcjonariusze wywiadu tego kraju, a sam Pegasus uznawany jest przez wielu za groźną broń, to może warto było jakoś instytucjonalnie kontrolować, komu oprogramowanie jest sprzedawane i unikać sytuacji, w których wpada ono w ręce reżimów nadużywających szpiegostwa elektronicznego wobec

własnych obywateli? Takie ryzyka istnieją też w Polsce i, jak sądzę, Tel Awiw jest tego świadomy. Może jednak nie ma instrumentów monitoringu i kontroli transakcji, choć nie bardzo chce się w to wierzyć.

– Są przecież jednak instrumenty prawne ograniczające praktyki inwigilacji.

– Myślę, że po pierwsze (co potwierdzają polscy prawnicy) – kontrola sądowa nad stosowaniem inwigilacji jest oparta o przepisy niedostosowane do współczesnych realiów technologicznych. Po drugie – wymóg kontroli sądowej jest często omijany przez służby, a sytuację taką usankcjonował już w roku 2016 Zbigniew Ziobro, wprowadzając nowelizację Kodeksu postępowania karnego, która umożliwia wykorzystywanie w postępowaniu sądowym materiałów zdobytych w sposób nielegalny, np. nagrań czy zapisów. Po trzecie – nie wszystkim sędziom udaje się uniknąć podejścia, by dla świętego spokoju zatwierdzać wszystkie wnioski prokuratury czy służb, szczególnie w tych ciężkich dla wymiaru sprawiedliwości czasach.

– Wicepremier Jacek Sasin stwierdził jednak, że „jak ktoś nie ma nic do ukrycia, to się nie ma czego obawiać", uspokajał opinię publiczną.

– Trudno to komentować. Mój przyjaciel, który był represjonowany politycznie w okresie stanu wojennego stwierdził, że to retoryka żywcem wzięta z tamtego okresu. Minister Sasin też nie powinien być tak pewien, że nie ma się czego bać, choćby dlatego, że (jak pokazuje praktyka) jego partyjni koledzy kontrolujący służby specjalne mogą zbierać potencjalne haki także na niego, a nuż w przyszłości się przydadzą. Podejście zaprezentowane przez Jacka Sasina jest absurdalne, bo chyba nie ma na świecie państwa, którego obywatele mają przekonanie, że można w 100% ufać w czystość intencji kontrolowanych przez rządzących polityków służb specjalnych. Taka sytuacja jest teoretycznie możliwa, albo w

państwie totalitarnym, którego obywateli poddano indoktrynacji graniczącej z lobotomią, albo w jakimś państwie rodem z marzeń utopistów. Nie jest możliwa natomiast w najmniejszym nawet stopniu w kraju takim, jak Polska, w którym – jak twierdzą najlepsi politologowie – ma obecnie miejsce przyspieszona ewolucja w kierunku autorytaryzmu.

– Jakie mogą być skutki polityczne znalezienia się w rękach służb takiego szpiegowskiego oprogramowania?

– Krótkookresowe być może pojawią się już w czasie kampanii wyborczej, jeśli ktoś zdecyduje się tego systemu użyć, chociaż – jak sądzę – PiS może spokojnie wygrać wybory bez specjalnych spektakli medialnych przeciwko opozycji. Wiadomość o inwigilacji nie spowodowała też jakiegoś spadku notowań partii rządzącej, bo jej elektorat raczej w świecie cyfrowym odnajduje się słabo. Średniookresowo – dojdzie do jeszcze większej brutalizacji polityki, której ofiarą padać będą nie tylko politycy opozycji, ale też zapewne na pewnym etapie również politycy obozu rządzącego w ramach wewnętrznych wojen i porachunków. Długookresowo – mamy do czynienia z rozbudową instrumentarium reżimu autorytarnego, z sytuacją, w której obecny autorytaryzm operetkowy, momentami bardzo nieudolny, sprofesjonalizuje się. Oznacza to postępujące ograniczanie wolności i swobód obywatelskich, aż do zamrożenia jakiejkolwiek działalności rzeczywiście opozycyjnej. To nie będzie już kraj dla ludzi myślących własnym rozumem.

– Bardzo dziękuję za rozmowę.

Oświadczenie CBA

Wydział Komunikacji Społecznej CBA na oficjalnej stronie CBA opublikowało oświadczenie w tej sprawie: „W związku z doniesieniami mediów informujemy, że Centralne Biuro Antykorupcyjne prowadzi swoje działania w oparciu o przepisy polskiego prawa. Kontrola operacyjna jest prowadzona w uzasadnionych i opisanych prawem przypadkach, po uzyskaniu

zgody Prokuratura Generalnego i wydaniu postanowienia przez sąd. CBA nie zakupiło żadnego „systemu masowej inwigilacji Polaków”. Pojawiające się w tej sprawie opinie i komentarze są insynuacjami i nie mają poparcia w faktach.”

Z Mateuszem Piskorskim rozmawiał Igor Stanow
Źródło: pl.SputnikNews.com