aut. Andrzej Kozłowski 14.08.2020

MINISTER CYFRYZACJI: ZARZUTY WOBEC APLIKACJI PROTEGO SAFE SĄ CAŁKOWICIE NIEUZASADNIONE [WYWIAD]

„Ataki i krytyka ProteGo Safe, oraz oskarżenia, że za jej pomocą chcemy inwigilować obywateli są niedorzeczne, trudno się nam przed takimi zarzutami bronić" – stwierdził minister Marek Zagórski. W wywiadzie, szef resortu cyfryzacji mówił również o wyznaczonych przez ministerstwo kierunkach rozwoju Krajowego Systemu Cyberbezpieczeństwa, pomocy dla samorządów w obszarze poniesienia poziomu cyberbezpieczeństwa oraz przyszłości programu Partnerstwo dla Cyberbezpieczeństwa.

Jaką rolę odegrały nowoczesne technologie w walce z pandemią koronawirusa?

Mamy narzędzia, które bezpośrednio wspomagają funkcjonowanie służb odpowiedzialnych za walkę z pandemią. Przykładem jest aplikacja „Kwarantanna Domowa" czy też oprogramowanie analityczne, które pozwala na predykcję rozwoju COVID-19 w celu lepszego planowania procesu zaopatrzenia placówek służby zdrowia czy też monitorowania mobilności Polaków w oparciu o anonimowe dane operatorów telekomunikacyjnych. Dzięki czemu możliwe było podniesienie skuteczności służb sanitarnych, pozwalając im na monitorowanie osób, które np. wyjechały z miejsca, gdzie pojawiło się ognisko koronawirusa.

Posiadamy również narzędzia informatyczne, które pomagały bezpośrednio w funkcjonowaniu gospodarki, państwa i administracji. Ponadto bez usług takich jak profil zaufany, gov.pl nie bylibyśmy gotowi, aby przenieść tak wiele działań administracji do sieci i umożliwić obywatelom korzystanie z e-usług, z czego zresztą nasi rodacy korzystali w czasie pandemii na dużą skalę.

Wreszcie mamy wszystkie inne usługi, które oferuje biznes, w tym przede wszystkim wykorzystanie usług chmurowych, co pozwoliło na szybkie dostosowanie wydajności poszczególnych systemów do zwiększonego zainteresowania i dużo większej liczby klientów.

Jednym z ważniejszych elementów w walce z koronawirusem były i są aplikację śledzące kontakty międzyludzkie. Czy Pana zdaniem aplikacja ProteGO Safe odniosła sukces? Liczba osób, która ściągnęła tę aplikację jest niewielka i zdecydowanie nie udało się przekroczyć progu, kiedy to 60 % całego społeczeństwa miałoby ją w swoim smartfonie. Próg ten jest uważany przez ekspertów za konieczny do osiągnięcia, żeby mówić o skuteczności takich działań?

Obecnie mamy niemal 500 tys. osób, które pobrały tę aplikację, co oczywiście jest dalece niewystarczające, żeby osiągnąć ten próg, który w wypadku Polski wynosi kilka milionów. W Niemczech dokładnie taką samą aplikację, która niczym się nie różni od polskiej, w kwestii ochrony danych osobowych, bezpieczeństwa i ochrony prywatności, w pierwszych dniach ściągnęło 6.5 mln osób, a obecnie ponad 10 mln. Ta aplikacja jest potrzebna. Nie nastawialiśmy się na bardzo szybki i

spektakularny przyrost liczby użytkowników, dlatego, że w Polsce to trochę inaczej działa. Zakładaliśmy, że będziemy mieli stopniowy wzrost, tak aby osiągnąć kilka milionów użytkowników przed spodziewanym jesienią nawrotem pandemii.

Warto jednocześnie podkreślić, że masowe korzystanie z aplikacji to szansa na ograniczenie rozprzestrzeniania się koronawirusa, ale nie oznacza to, że aplikacja nie jest skuteczna w sytuacji gdy korzysta z niej mniejsza liczba osób. Już dzisiaj przy pół milionie użytkowników generowane są ostrzeżenia, są osoby, które dzięki aplikacji dowiedziały się, że miały kontakt z osobami zarażonymi.

Jakie działania zamierzają Państwo podjąć, aby promować aplikację w społeczeństwie oraz żeby rozwiać kontrowersje, które pojawiły się w mediach?

Mamy przygotowaną kampanię medialną, za nami jej pierwszy etap, m.in. emisja spotów telewizyjnych, działania w prasie i internecie. W kolejny etapie także będziemy prowadzić działania na wielu polach. Reagujemy na bieżąco, wsłuchujemy się w głosy i wątpliwości Polaków i na tej podstawie m.in. korygujemy język tej kampanii, większy nacisk kładziemy na praktyczne zastosowanie tego rozwiązania, zamiast tylko w ogóle informować o takiej aplikacji. Konieczne jest wyjaśnienie w prosty i zrozumiały sposób mechanizmów jej działania. Uważam, że to główna bariera przed jej instalacją.

Odnosząc się do kontrowersji to muszę przyznać, że spotkaliśmy z kompletnie niesprawiedliwymi zarzutami, jeśli chodzi o to rozwiązanie. Pracę nad ProteGO Safe rozpoczęliśmy jako jedno z pierwszych państw w Europie, w sytuacji, w której nikt nie miał do końca sprecyzowanej wizji jak taka aplikacja w ogóle powinna wyglądać.

Kiedy zaczęliśmy nad nią pracę, to nikt nie słyszał o tym, że Google i Apple przedstawiają własny interfejs powiadomień o narażeniu na kontakt z koronawirusem. Mówiło się o modelu częściowo zdecentralizowanym, a model całkowicie zdecentralizowany był na poziomie prac koncepcyjnych. Cały proces prac nad aplikacją miał charakter projektu badawczo-rozwojowego, w którym zmienialiśmy różne szczegółowe rozwiązania bazując na tym, co sami odkryliśmy, ale także zbierając informacje z całego świata.

Kiedy okazało się, że Singapur jako pierwszy uruchomił aplikację do monitorowania koronawirusa i udostępnił kod źródłowy, od razu postanowiliśmy część tych rozwiązań zaadaptować. Po zapowiedzi zbudowania rozwiązania przez Google i Apple również postanowiliśmy się do tego włączyć. W połowie kwietnia nie wiedzieliśmy jeszcze, kiedy rozwiązania amerykańskich firm zostaną dostarczone, więc pracowaliśmy nad swoimi, jednocześnie wykazując się maksymalną transparentnością. Możemy powiedzieć, że dzisiaj nasza aplikacja opiera się nie tylko na API Apple i Google, ale przede wszystkim mieliśmy duży wkład na to jak te rozwiązania ostatecznie wyglądają. Cały czas blisko współpracowaliśmy i współpracujemy z inżynierami tych koncernów.

Co do zarzutów - spotkaliśmy się z m.in. takimi, że chcemy inwigilować obywateli, co jest całkowitą nieprawdą. Takie oskarżenia wynikały z tego, że byliśmy jednym z pierwszych państw pracujących nad koncepcją takiej aplikacji. Cały czas wybieraliśmy jednak takie rozwiązania, które będą w jak najmniejszym stopniu ingerować w prywatność. Właśnie w ten sposób ostatecznie doszliśmy do rozwiązania, które dzisiaj mamy.

Chcę podkreślić, że nie wszystkie państwa w Europie zdecydowały się na rozwiązania w tak dużym stopniu chroniące prywatność. Brytyjczycy wprowadzili początkowo model scentralizowany, z którego ostatecznie się wycofali, podobnie Norwegowie, których aplikacja działa w oparciu o lokalizacje na GPSie, więc ingerowała w prywatność jeszcze bardziej niż rozwiązanie brytyjskie. Też się z niego w końcu wycofano. Francja wypuściła aplikację, która ma charakter scentralizowany, a dane są

zapisywane nie tylko na urządzeniach użytkowników, ale również na serwerach rządowych. Polska podobnie jak większość państw europejskich przyjęła model zdecentralizowany oparty o API Google i Apple. Jesteśmy jednym z pierwszych krajów, który rozpoczyna pracę nad rozwiązaniem gwarantującym interoperacyjność tej aplikacji, żeby była użyteczna np. przy wyjeździe na wakacje. Podjęliśmy również współpracę z Niemcami, aby niemieckie i polskie rozwiązania mogły się ze sobą komunikować.

Odwołujemy się do przykładów Niemiec, Francji czy Włoch, żeby pokazać, że w tamtych społeczeństwach, równie wrażliwych na kwestie prywatności i bezpieczeństwa danych jak w Polsce, funkcjonują bardzo podobne aplikacje, które traktowane są jako przydatne narzędzia.

Ataki i krytyka ProteGo Safe oraz oskarżenia, że za jej pomocą chcemy inwigilować obywateli są niedorzeczne, trudno się nam przed takimi zarzutami bronić, bo ciężko jest dyskutować, kiedy ktoś nie chce zobaczyć jak to faktycznie działa. Powołaliśmy zespół ekspertów, do którego zaprosiliśmy przedstawicieli wielu organizacji takich jak np. Panoptykon. Cały czas pracujemy nad tym, aby ta aplikacja była jak najbardziej restrykcyjna, czyli żeby nie było możliwości w jakimkolwiek stopniu ujawnienia danych obywateli. Zrobiliśmy wiele, by udowodnić to, że nie mamy absolutnie nic do ukrycia, np. opublikowaliśmy ocenę ryzyka. Zależy nam, aby wszyscy zrozumieli, że jedyną intencją rządu w tej sprawie jest udostępnienie narzędzia, które pozwoli nam lepiej funkcjonować w obecnej sytuacji.

Pewnym problemem okazało się również to, że nasza aplikacja była gotowa wtedy, kiedy zdejmowaliśmy największe ograniczenia w związku z pandemią. W społeczeństwie pojawiło się wówczas d poczucie, że epidemia się skończyła. Już wiemy, że jest inaczej. Zmienia się w związku z tym podejście do środków ochrony, w tym do takich jak aplikacja. Widzimy tego efekty w przyroście użytkowników ProteGO Safe. W trakcie ostatnich 7 dni aplikację pobrało ponad 140 tysięcy osób.

Czas pandemii to również wzmożona aktywność cyberprzestępców a to z kolei generuje wyzwania dla cyberbezpieczeństwa. Jak program „Partnerstwo dla Cyberbezpieczeństwa" funkcjonuje w czasach pandemii i jakie korzyści przynosi?

To nie tylko ten jeden program, ponieważ trzeba pamiętać, że podpisaliśmy porozumienie z operatorami telekomunikacyjnymi w sprawie stworzenia listy ostrzeżeń, w ramach której nasi partnerzy zobowiązali się do zgłaszania stron internetowych i aplikacji wyłudzających dane. Cyberprzestępcy bardzo chętnie wykorzystywali poczucie strachu - zwłaszcza w pierwszym okresie pandemii. W ramach tej listy do tej pory zgłoszono ponad trzy tysiące stron, które zostały zablokowane. Jeśli chodzi o „Partnerstwo dla Cyberbezpieczeństwa", to jednym z elementów programu jest wymiana informacji o różnego rodzaju zagrożeniach, których - ze względu na pandemię - było o wiele więcej. Zaczęło się od oszustw i sprzedawania produktów, które mają mieć cudowne właściwości zwalczania koronawirusa, jak np. mydło, które na platformach sprzedażowych oferowano za 300 zł. Były również próby wyłudzania pieniędzy poprzez podszywanie się pod różnego rodzaju instytucje jak np. Ministerstwo Zdrowia. Zaobserwowaliśmy również wzrost akcji phisingowych, które staraliśmy się łagodzić poprzez współpracę i wymianę informacji na temat incydentów i ataków, które miały miejsce na całym świecie.

Czy program „Partnerstwo dla Cyberbezpieczeństwa" będzie w przyszłości dostępny dla innych państw niż członkowie UE, NATO i partnerów tych organizacji?

Na tym etapie nie. Chcemy, aby ten program był atrakcyjny dla wszystkich stron w nim uczestniczących. Jego zaletą będzie wymienianie danych, w tym informacji poufnych. Przystępując do programu, każdy członek, chce mieć gwarancje, że współpraca będzie się odbywała w ramach pewnego poziomu zaufania i dlatego nie przewidujemy rozszerzenia tego programu o podmioty inne

niż te pochodzące z krajów należących do UE, NATO oraz państw będących partnerami tych organizacji.

Za rok czy dwa dokonamy podsumowania i wtedy wspólnie z partnerami zdecydujemy czy jest potrzeba jego rozszerzenia. Chcę zwrócić uwagę, że jednym z elementów Programu jest współpraca SOCów. Dlatego musimy dopracować, jak wygląda wymiana informacji w tym programie. Im węższy krąg podmiotów w ramach Partnerstwa dla Cyberbezpieczeństwa, tym większe jest bezpieczeństwo przekazywanych informacji. Dopóki nie zamkniemy pierwszego etapu to trudno jest mówić o dalszych krokach.

Krajowy System Cyberbezpieczeństwa jest fundamentem cyberbezpieczeństwa w Polsce. Jakie będą kierunku rozwoju KSC w przyszłości?
Po pierwsze będziemy chcieli zintensyfikować proces powstania CSIRTów sektorowych. To się już dzieje. Taki zespół powstał przy Komisji Nadzoru Finansowego (KNF). Są kolejne propozycje od ministrów w sektorach szczególnie dla nas istotnych. Chcemy również przedłożyć zmiany w ustawie o KSC w celu modyfikacji niektórych elementów. Część z tych zagadnień jest związana z bezpieczeństwem sieci telekomunikacyjnych. Procedura uznania, że dostawca jest dostawcą wysokiego ryzyka powinna mieć swoje umocowanie ustawowe. Będziemy chcieli doprecyzować istniejące delegacje ustawowe przy okazji nowelizacji ustawy o KSC i zmianie prawa telekomunikacyjnego. W tej chwili pracujemy nad implementacją europejskiego kodeksu łączności elektronicznej, co spowoduje, że prawo komunikacji elektronicznej zastąpi prawo telekomunikacyjne. Nasz projekt jest już w konsultacjach. Będziemy dążyli do stanu, aby precyzja przepisów była coraz większa. Chciałbym również wzmocnić system poprzez utworzenie Krajowego Centrum Analitycznego. Zamierzamy ustanowić jednostkę koordynowaną na poziomie pełnomocnika ds. cyberbezpieczeństwa, nazywaną Krajowym Centrum Analitycznym, gdzie zgromadzimy najwyższej klasy specjalistów w zakresie cyberbezpieczeństwa.

Jednym z największych wyzwań, jeżeli chodzi o cyberbezpieczeństwo są samorządy. Ministerstwo Cyfryzacji ruszyło z kampanią cyberbezpieczny samorząd. Co ona zakłada i jakie są jej cele?

Najpierw musimy zbudować świadomość w zakresie cyberbezpieczeństwa i to pierwszy i najdalej idący cel, czyli zbudowanie odpowiednich kompetencji urzędników na poziomie podstawowym. Chcemy przeszkolić wszystkich urzędników w Polsce z podstawowych zasad cyberhigieny. Zamierzamy również przeszkolić osoby, które są odpowiedzialne za bezpieczeństwo i funkcjonowanie sieci i systemów informatycznych w poszczególnych jednostkach administracji publicznej, aby wyposażyć je w większe kompetencje. Chcemy także zaprojektować system wsparcia dla samorządów polegający na ułatwieniu im dotarcia do ekspertów i korzystania z ich wiedzy. Pamiętajmy, że ekspertów od cyberbezpieczeństwa jest ogólnie niewielu, a ich pozyskanie przez małą gminę jest praktycznie niemożliwe. Dlatego chcemy, aby powstały regionalne centra kompetencji cyberbezpieczeństwa, które będą wspomagały prace samorządów. Zamierzamy również przygotować dedykowane narzędzia. Pierwszym z nich jest uchwała Rady Ministrów o wspólnej infrastrukturze informatycznej państwa. Chcemy także umożliwić korzystanie z usług dostawców chmurowych przez jednostki administracji - w tym samorządy. Co do zasady takie rozwiązania już same z siebie zwiększają poziom bezpieczeństwa. Obserwując ataki na samorządy w ostatnich latach widzimy, że słabością są ich strony internetowe oraz systemy poczty elektronicznej. Będziemy im oferować dobrowolne narzędzia, np. będziemy chcieli niejako „skopiować” gov.pl i dostarczyć to rozwiązanie samorządom, po to, żeby mogły korzystać z takiej samej infrastruktury do swoich własnych potrzeb.

Podsumowując, rozpoczęliśmy już działania edukacyjne i informacyjne i chcemy je prowadzić na dużo większą skalę niż kiedykolwiek to się odbywało. Zamierzamy też zapewnić opiekę instytucjonalną w postaci dostępu do specjalistów i wiedzy oraz wyposażyć w narzędzia zachęcające do korzystania za

usług chmury publicznej, a ostatecznie przygotować gotowe narzędzia jak np. samorzad.gov.pl.

Panie Ministrze przejął pan obowiązki pełnomocnika rządu ds. cyberbezpieczeństwa. Jak Pan sobie wyobraża łączenie tych dwóch stanowisk i jaka jest Pana wizja na cyberbezpieczeństwo w Polsce?

Rolą pełnomocnika jest koordynowanie działań podejmowanych przez różne instytucje w Polsce w zakresie cyberbezpieczeństwa. Jest odpowiedzialny za wynikające z przepisów zadania formalne, takie jak np. wydawanie rekomendacji, współpraca z kolegium ds. cyberbezpieczeństwa, ministrami wiodącymi i szefami CSIRTów. Chciałbym, aby te zadania były systematyczne i rutynowe. Druga kwestia to stałe monitorowanie i rozbudowywanie systemu Krajowego Systemu Cyberbezpieczeństwa. Zamierzam również wzmacniać programy takie jak Partnerstwo dla Cyberbezpieczeństwa oraz stawiać na edukację i podnoszenie kompetencji zarówno, jeśli chodzi o specjalistów funkcjonujących w administracji, jak również urzędników oraz społeczeństwo. Bardzo ważna jest tzw. cyberhigiena. Musimy pamiętać też o miękkim zagrożeniu, czyli dezinformacji, która mieści się w obszarze cyberbezpieczeństwa i tutaj najlepszym narzędziem jest wiedza i kompetencje ogółu społeczeństwa.

Podstawowym celem, który sobie stawiam, jest rozbudowa systemu w różnych warstwach, o których powiedziałem: zdolność instytucji do tego, żeby przeciwdziałać zagrożeniom i związane z tym działania takie jak rządowa chmura czy klaster bezpieczeństwa.

Jesteśmy na etapie kończenia prac nad nową architekturą systemów rządowych i potrzebna jest rozbudowa CSIRTów sektorowych, lepsza koordynacja i współpraca z biznesem. Jest mnóstwo rzeczy do zrobienia, np. poprawienie niedoskonałości, które pojawiają się w samorządach. Zmagamy się z coraz większą liczbą cyberataków co jest konsekwencja zwiększonej aktywności w cyberprzestrzeni