STREŻYŃSKA DLA CYBERDEFENCE24.PL: CYBERBEZPIECZEŃSTWO MA CHARAKTER CYWILNY

O rządowych planach i priorytetach wzmocnienia cyberbezpieczeństwa – mówi w wywiadzie dla Cyberdefence24 minister cyfryzacji Anna Streżyńska.

Na cztery dni przed szczytem NATO dokonała Pani otwarcia Narodowego Centrum Cyberbezpieczeństwa w NASK, który jako instytut naukowo-badawczy podlega nadzorowi Ministra Cyfryzacji. Czy jest już kandydat na szefa tej jednostki?

To musi być staranny wybór. Szefem powinien zostać ktoś o ogromnej wiedzy i umiejętności połączenia wszystkich kompetencji, które ma ta instytucja, również w środowiskach eksperckich. Nie chodzi tu wcale o specjalistę od bieżącej działalność operacyjnej, bo tą w ramach NC Cyber zajmuje się już CERT Polska, który ma swojego szefa.

Krążyła wcześniej informacja, jakoby na czele NC Cyber miał stanąć Jacek Wojtala, który przyszedł do NASK z ZUS, a wcześniej przez całe lata służył w Wojsku Polskim m.in. specjalizując się w systemach walki radioelektronicznej.

Pan Jacek Wojtala został specjalnie ściągnięty do NASK, żeby przyspieszyć prace nad uruchomieniem NC Cyber. To człowiek pełen niespożytej energii. Wiedzieliśmy w ministerstwie, że sprawnie zepnie wszystkie nitki między bankami, telekomami i innymi instytucjami rynkowymi, które włączyły się w projekt budowy NC Cyber. Jego wiedza i energia są też istotne w dalszym rozwoju tej jednostki.

Jak uruchomienie tej jednostki może wpłynąć na zwiększenie bezpieczeństwa kraju w cyberprzestrzeni?

To jest plan długookresowy. Jako minister właściwy do spraw informatyzacji mam – zgodnie z ustawą działową – ustawowo przypisane cyberbezpieczeństwo jako zadanie. Z drugiej strony w NASK od dawien dawna działał renomowany zespół CERT Polska, który ma naprawdę dobrych analityków. Zawsze mi tam jednak brakowało ramienia eksperckiego, które gromadziłoby doświadczenia i dystrybuowało je po innych instytucjach zajmujących się cyberbezpieczeństwem. Potrzebne było stworzenie łącznika, platformy edukacyjnej czy wręcz zaplecza ekspercko-badawczego, które umożliwiałoby zorientowanie się, co dzieje się po drugiej stronie bariery, czyli wśród tych, którzy dokonują ataków. Stąd wziął się pomysł, żeby ściągnąć z różnych miejsc ludzi, którzy znają się na cyberbezpieczeństwie. Pochodząca z rynku wiedza, zebrana w jednym ośrodku, pozwoli zbudować zaplecze nie tylko dla Ministerstwa Cyfryzacji, ale również dla całego rządu i dla tych wszystkich instytucji czy firm, które postanowiły się akredytować przy CERT Polska, stanowiącym teraz – jako CERT Narodowy – część NC Cyber.

Co dla Pani stanowi najcenniejszy element tej nowej koncepcji, którą urzeczywistnić ma NC Cyber?

Radykalnie wzmocniony został pion cyberbezpieczeństwa. Kluczowe znaczenie ma obecność przedstawicieli kilkunastu wiodących firm i instytucji rynkowych, które się akredytowały przy NC Cyber. To właśnie w sieciach biznesowych, infrastrukturach krytycznych, najszybciej i najgroźniej ujawnia się większość cyberzagrożeń. Wymiana informacji w NC Cyber między przedstawicielami biznesu reprezentującymi różne sektory gospodarki, każdy o innej specyfice takiej jak infrastruktura krytyczna (transport, energia, telekomy, IT, banki), a instytucjami takimi jak ZUS czy inne organy administracji publicznej, pozwala na szybkie reagowanie na zagrożenia i incydenty. Przetestowaliśmy już skuteczność tego systemu wprowadzając program 500+. Przyjęte wtedy założenia, które teraz zostały wykorzystane w NC Cyber, umożliwiły przeciwdziałanie cyberzagrożeniom w czasie mierzonym w minutach. Bezcenną wartość w NC Cyber stanowi ponadto możliwość wymiany doświadczeń i wejrzenia nawzajem do swoich, niedostępnych w innych okolicznościach światów. To pozwala tym, którzy ich nie widzieli z bliska, zobaczyć jak one funkcjonują. Ma to szczególne znaczenie dla administracji, która póki co może jedynie uczyć się od biznesu. On już odrobił tę lekcję.

Jaką rolę wobec administracji publicznej Ministerstwo Cyfryzacji widzi dla NC Cyber z jego CERT Narodowym?

O ile sam CERT bez przerwy monitoruje sieć, to w NC Cyber we współpracy z Ministerstwem Cyfryzacji będą powstawały koncepcje zabezpieczeń dla administracji państwowej. Ich brak wielokrotnie sygnalizowałam odwołując się m.in. do dwóch raportów Najwyższej Izby Kontroli obnażających poziom indolencji administracji w zakresie cyberbezpieczeństwa. Pomału, krok po kroku namawiamy kolejne resorty, żeby we współpracy z nami zbudowały sobie odpowiednią strukturę i dołączały do klastra bezpieczeństwa dla administracji. Wprowadzi on w administracji pewne modyfikacje do otwartego obiegu informacji, który jest nacechowany brakiem odporności. W ramach klastra bezpieczeństwa zamierzamy zorganizować zarówno komunikację, jak i zasady obrony przed ewentualnymi zagrożeniami zewnętrznymi.

Czy Narodowe Centrum Cyberbezpieczeństwa będzie współpracować przy realizacji projektu Cyberpark Enigma, o którym kilka miesięcy temu mówił wicepremier - minister rozwoju Mateusz Morawiecki?

Nie znam odpowiedzi na to pytanie. Mówimy o projekcie, który jest realizowany przez wicepremiera - ministra rozwoju wspólnie z ministrem obrony narodowej.

Jak osiągnąć cel związany z cyberbezpieczeństwem w państwie zorganizowanym silosowo, w którym każdy minister czy szef organu administracji jest udzielnym panem w swoim księstwie?

Program 500+ pokazał, że najlepszym rozwiązaniem tego problemu jest współpraca, której efekty już są widoczne. Wszystkie resorty, zarówno wiodące w tej dziedzinie, jak i te, które jedynie muszą zachować bezpieczeństwo, są zmuszone, żeby ze sobą współpracować. Każdy ma swoje zadania i jakąś ważną rolę do odegrania. Poza Ministerstwem Cyfryzacji, które pełni rolę koordynującą i realizuje zadania wynikające z ustawy działowej, mamy jeszcze trzy inne organy, w których obszarze działalności znajdują się zadania z zakresu cyberbezpieczeństwa. Są to MON, MSWiA z Policją i ABW. Do MON należą wszystkie kwestie związane z obroną i zagrożeniami zewnętrznymi, do MSWiA – zagrożenia przestępcze i naruszenia prawa (te wątki zwykle „kończą się” u ministra sprawiedliwości), a do ABW – ochrona infrastruktury krytycznej i państwowej. Trwają nieustanne rozmowy z tymi trzema kluczowymi resortami. Poza tym są jeszcze: BBN (doktryna obronna), KNF, NBP i wiele wspomagających instytucji. Z rozmów i uzgodnień wynika, że konieczne jest wskazanie, kto za co odpowiada. Następnie należy ująć całość problematyki w ramy wspólnego planu czy strategii i wreszcie zapewnić infrastrukturę, która będzie gwarantować bezpieczeństwo. Korespondując z różnymi organami otrzymaliśmy wiele ciekawych sygnałów jak poszczególne ministerstwa i urzędy

wyobrażają sobie tę współpracę i korzystanie z infrastruktury czy narzędzi zapewniających cyberbezpieczeństwo. Na początku mieliśmy spotkanie, na którym wszystkie uwagi zostały przedyskutowane; przed nami szereg kolejnych rozmów. Myślę, że na koniec roku będziemy mieli poukładaną strukturę i być może także możliwość sprawdzenia na ćwiczeniach jak to wszystko funkcjonuje w praktyce. I co najważniejsze, będzie też gotowy dokument – projekt ustawy o cyberbezpieczeństwie.

Niedawno przewodniczący Sejmowej Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii Paweł Pudłowski z klubu Nowoczesna w interpelacji do ministra obrony narodowej zapytał, jaki jest przepływ informacji pomiędzy MON a Ministerstwem Cyfryzacji w kontekście prac nad „Strategią cyberbezpieczeństwa dla RP".

MON był w tym procesie uczestnikiem konsultacji. Tak jak i wszystkie inne podmioty. Prowadziliśmy konsultacje publiczne i międzyresortowe. Wszyscy ministrowie mieli możliwość wypowiedzenia się, wpłynęły uwagi i są one implementowane.

Czy minister obrony to właściwy adresat sformułowanego w cytowanej interpelacji pytania: „Kiedy MON przygotuje stosowne dokumenty nadające bieg legislacyjny ustawie o cyberbezpieczeństwie Polski?".

MON nie jest organem właściwym w tym zakresie, ponieważ to jest właściwość ministra cyfryzacji. Te dokumenty – jak wcześniej wspomniałam – będą gotowe do końca roku. Nie ulega najmniejszej wątpliwości, że wątki cyberbezpieczeństwa pojawią się w obszarze wspólnym z Ministerstwem Obrony. Jako Ministerstwo Cyfryzacji posiadamy rozległe kompetencje: to minister właściwy w sprawach informatyzacji odpowiada przecież za dostarczenie łączności na potrzeby obronności państwa. Zobowiązany jest także w ustawie o obronności do przygotowania dokumentów krajowego systemu łączności na potrzeby bezpieczeństwa. Nota bene, właśnie skończyliśmy nad nim pracę i został rozesłany do uzgodnień międzyresortowych. Mamy szereg obowiązków względem podlegających nam instytucji, zwłaszcza operatorów telekomunikacyjnych, z którymi podpisujemy umowy o świadczeniu służebności wobec państwa związanych z obronnością, jak również wydajemy w tym zakresie decyzje. Reasumując: piszemy teraz ustawę o cyberbezpieczeństwie i kiedy projekt będzie już gotowy, wszystkie strony będą mogły dodać coś od siebie, żeby zabezpieczyć własne potrzeby i interesy.

Uzgodnienia międzyresortowe i pozostałe prace nad ustawą o cyberbezpieczeństwie zbiegają się akurat z zapowiedzianym procesem sprzedaży przez PGE Polską Grupę Energetyczną operatora teleinformatycznego Exatel. Jego przyszły właściciel Polska Grupa Zbrojeniowa chce, by Exatel odegrał wiodącą rolę w rozwoju segmentu cybertechnologii grupy kapitałowej kontrolowanej przez Skarb Państwa.

Jako Ministerstwo Cyfryzacji poparliśmy takie rozwiązanie, kiedy były uzgodnienia międzyresortowe. Ten pomysł z wielu względów spotkał się z naszą pełną, absolutną wręcz aprobatą. Pierwszy i podstawowy powód ma związek z kondycją i wymaganiami tej spółki. Infrastruktura, którą Exatel dysponuje, jest wprawdzie rozległa, ale niejednolita i w większości nie należy do tej spółki. Zaledwie jedna trzecia infrastruktury Exatela jest rzeczywiście jego własnością. Część nie stwarza niezbędnych warunków bezpieczeństwa, gdyż jest podwieszona na słupach energetycznych. A jedna trzecia jest dzierżawiona od innych operatorów, w tym oczywiście od naszego kluczowego operatora (Orange – dawna Telekomunikacja Polska S.A.). W takich warunkach trudno mówić o jakiejś spójnie zbudowanej sieci. Rozmawialiśmy wielokrotnie z Exatelem i poprzedni zarząd spółki prezentował nam jej możliwości, jeśli chodzi o dostarczanie usług. Exatel dostarcza je administracji prowadząc sieci Gov.net (dla administracji państwowej) i OST 112 (na potrzeby obsługi numeru alarmowego), ale nie jest w stanie dostarczać np. usług dla klientów końcowych takich jak np. jednostki samorządu

terytorialnego, terenowa administracja państwowa, placówki służby zdrowia, banki czy instytucje użyteczności publicznej. Pokazywano nam wiele perspektywicznych usług, które mogłyby być świadczone przez sieć Exatela, ale spośród nich zaledwie kilka może być obecnie dostarczanych użytkownikom końcowym z uwagi na niedostatecznie rozwiniętą sieć lokalną. To oznacza, że spółka potrzebuje dużych inwestycji, żeby stać się operatorem teleinformatycznym, jakiego potrzebuje administracja.

Już jakiś czas temu była o tym mowa w Sejmie.

To prawda. W grudniu ub.r. na posiedzeniu Sejmowej Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii przekonywałam posłów, że Exatel mógłby stać się takim zaczątkiem infrastruktury państwowej. I cały czas obstaję przy tym poglądzie. Przy czym należy zaznaczyć, że dzisiaj spółka nie ma niezbędnego potencjału. Ten potencjał jest naturalnie do zbudowania, ale minister cyfryzacji nie ma pieniędzy na taką inwestycję. Zasygnalizowałam wcześniej zainteresowanie nową rolą dla tego operatora teleinformatycznego ministrowi Skarbu Państwa i bardzo się teraz cieszę, że wreszcie znalazł się ktoś, kto nie tylko rozumie tę potrzebę państwa, ale ma też niezbędny potencjał, by stworzyć Exatelowi odpowiednie możliwości działania. Dla mnie to jest również dobra nowina dlatego, że Exatel zbudował Security Operations Center (SOC), bodaj najnowocześniejszy w kraju, który zbiera same pochwały i teraz przygotowuje się do realizacji strategicznych zadań związanych z zapewnieniem cyberbezpieczeństwa. Im więcej takich jednostek, tym lepiej. Administracja bardzo potrzebuje nowoczesnych zabezpieczeń i bogatej oferty usług. Widzę więc same plusy w zapowiedzianej zmianie właściciela spółki Exatel, a zmiana ta oznacza też jeszcze lepsze usługi dla dotychczasowego klienta, czyli energetyki.

Ta spółka jako operator teleinformatyczny już odegrała szczególną rolę w organizacji zakończonego właśnie Szczytu NATO w Warszawie.

Aktywność Exatela i jego zadania znajdowały się w gestii resortów, które odpowiadały za organizację i zabezpieczenie szczytu.

Operator teleinformatyczny świadczący specjalne usługi państwu kojarzy się też z szyfrowaną łącznością rządową. Czy minister cyfryzacji używa systemu CATEL do wymiany informacji poufnych, opracowanego przez kryptologów ABW?

Nie mam codziennej potrzeby, by go używać. Pamiętać trzeba, że większość działań administracji jest i powinna być po prostu jawna.

Czy to nie jest trochę Pani rola jako ministra cyfryzacji, żeby pozostałym ministrom i ważnym przedstawicielom państwa dawać wzór najlepszych praktyk, ucząc ich jak bezpiecznie korzystać z Internetu używając smartfonów, tabletów i mediów społecznościowych?

Zdecydowanie tak. Przede wszystkim uważam, że kluczowe jest odseparowanie łączności służbowej od prywatnej. Oczywiście wszyscy używamy smartfonów, powstaje jednak pytanie w jakim celu i jakiego rodzaju komunikacja odbywa się za ich pośrednictwem. Na całym świecie zdecydowana większość komunikacji między członkami rządu czy urzędnikami nie należy do kategorii niejawnej i nie stanowi tajemnicy przedsiębiorstwa czy tajemnicy kwalifikowanej. Ale oczywiście istnieją też dokumenty, które mają taki charakter. Dlatego szkoląc nowych pracowników informujemy ich jaki jest system tajemnic obowiązujących w administracji i w jaki sposób należy je chronić. Zarówno jeśli chodzi o dokumenty istniejące fizycznie, jak i elektroniczne. Trzeba to stale przypominać wyrabiając u urzędników nawyki odpowiedniego postępowania. Nie da się ukryć, że mamy łatwość, właściwie już odruch, używania mediów elektronicznych i na każdym urządzeniu konfigurujemy sobie własne konta.

Na szczęście funkcjonują kancelarie tajne, w których są udostępniane dokumenty zawierające informacje wrażliwe, zresztą najczęściej nie są udostępniane w formie elektronicznej, tylko na papierze. Sytuacja nie jest zatem zła i raczej nie można mówić o lekceważeniu problemu. Szkolenia są jednak potrzebne przez cały czas i na ten cel w ramach naszego projektu dotyczącego cyberbezpieczeństwa przewidziany jest duży moduł.

Skoro mowa o szkoleniu i świadomości zagrożeń wśród urzędników, to jak Pani ocenia taki oto fakt: szef Kancelarii Sejmu, piastujący to stanowisko od 2010 r., czyli z wieloletnim doświadczeniem, nie zgodził się na podłączenie do sejmowej sieci sondy cyberzagrożeń Arakis-GOV, mimo że żaden z organów władzy w państwie nie jest w stanie samodzielnie bronić się przed zagrożeniami ze strony hakerów? Tę sondę zaoferowała Sejmowi Agencja Bezpieczeństwa Wewnętrznego, która zbudowała ją wspólnie z NASK.

Nie wiem jakie były przyczyny takiej reakcji. Na pierwszy rzut oka może to wyglądać na lekceważenie zasad bezpieczeństwa, ale być może gdyby marszałkowie Sejmu i urzędnicy Kancelarii Sejmu zobaczyli jak działa to rozwiązanie, przekonaliby się, że warto je zainstalować, gdyż jest realnie potrzebne. Dotykamy tu kwestii braku świadomości i deficytu edukacji. Dlaczego w Kancelarii Sejmu tak postanowiono i czym się przy tym kierowano, tego oczywiście nie wiem, nie miałam możliwości zapoznać się z wyjaśnieniami urzędników sejmowych w tej sprawie. Takie problemy powinny być jednak uregulowane ustawowo. Osobiście uważam, że prawo powinno nakazywać administracji państwowej i podmiotom posiadającym elementy infrastruktury krytycznej instalowanie sond cyberzagrożeń. Wtedy nie będzie zbędnej dyskusji, a zabezpieczenia po prostu zostaną wprowadzone tam, gdzie są potrzebne.

Parę lat temu holenderski CERT zaalarmował swych polskich partnerów, że strona www Sejmu RP została zainfekowana i rozsiewa złośliwe oprogramowanie.

Wcale mnie to nie dziwi. Każdy komputer może zostać opanowany przez napastników. Strona sejmowa, sejmowe komputery i serwery nie są tu żadnym wyjątkiem. Nie przypadkiem cyberbezpieczeństwo ma charakter cywilny i zostało powierzone Ministrowi Cyfryzacji. W sektorach obronnych, administracyjnych czy infrastruktury krytycznej mamy pewnie setki tysięcy komputerów, ale u przedsiębiorców i obywateli jest ich kilkadziesiąt milionów. I to te, a nie inne urządzenia, są potencjalnie źródłem największych problemów, jako łatwiejsze do przechwycenia i wykorzystania do ataku na newralgiczne systemy krajowe. Szczególnie wrażliwe są sieci, w których funkcjonują zarówno urządzenia prywatne, jak i służbowe. Stąd tak dużą wagę przywiązujemy do budowania świadomości wśród obywateli. Wszyscy powinniśmy pamiętać o tych zagrożeniach, nie tylko korzystając z Internetu w pracy, ale także jako użytkownicy prywatni. To również może być droga ataku. Pojedynczy człowiek może tego nawet nie dostrzec.

Czy nie łatwiej byłoby uporządkować i koordynować całe spectrum funkcjonowania państwa i jego obywateli w cyberprzestrzeni, gdyby przy prezesie Rady Ministrów został powołany pełnomocnik ds. cyberbezpieczeństwa w randze podsekretarza czy nawet sekretarza stanu? Pełnomocnik, którego Pani powołała w Ministerstwie Cyfryzacji, nie ma tej rangi. Czy to nie utrudnia pracy?

W gruncie rzeczy umiejscowienie i ranga tego urzędnika są obojętne. Ważny natomiast jest zakres uprawnień i pełnomocnictw. Trzeba pamiętać, że jeden minister nie może nic narzucić innym ministrom. Członkowie rządu są wobec siebie równi. Dopiero ustawa przypisuje szefowi każdego z resortów pewne konkretne kompetencje, które umożliwiają oddziaływanie na określony rodzaj zadań innych ministrów. U nas zadania w zakresie cyfryzacji mają charakter horyzontalny. I tak, będąc ministrem cyfryzacji, działam jako główny informatyk kraju. Dzięki temu zbudowałam sobie narzędzia oddziaływania na innych ministrów i motywowania ich do racjonalizacji wydatków na cele

teleinformatyczne. Podobnie może to przebiegać w przypadku zadań z zakresu cyberbezpieczeństwa. Dotychczas żaden organ administracji nie odmawia współpracy z nami, mimo że uprawnień sformalizowanych w tej dziedzinie minister cyfryzacji nie ma. Natomiast w przyszłości, kiedy to będzie się wiązało z konkretnymi wydatkami i obowiązkami, zadania pełnomocnika do spraw cyberbezpieczeństwa zostaną na pewno uregulowane ustawowo. I stanie się tak niezależnie od tego, czy to będzie pełnomocnik rządu, pełnomocnik ministra czy sam minister.

Rozmawiał Jarosław Jakimczyk