aut. Andrzej Kozłowski 27.11.2018

CYFRYZACJA WCIĄŻ NIE JEST PRIORYTETEM. 3 LATA PIS W CYBERPRZESTRZENI [KOMENTARZ]

Uchwalenie Ustawy o Krajowym Systemie Cyberbezpieczeństwa to największy sukces 3 lat rządów PiSu w obszarze cyberbezpieczeństwa. Niestety inne ambitne projekty wciąż nie doczekały się realizacji. Najgorszą rzeczą jest jednak brak zrozumienia problemów cyberbezpieczeństwa i cyfryzacji państwa wśród najważniejszych polityków w państwie.

Trudne początki

W momencie objęcia władzy przez PiS polskie cyberbezpieczeństwo było w słabym stanie. Opublikowany w 2015 roku raport Najwyższej Izby Kontroli wskazywał na brak spójnych i systemowych działań w zakresie monitorowania i przeciwdziałania zagrożeniom występującym w cyberprzestrzeni. NIK wskazał również na paraliżowanie aktywności państwa w obszarze cyberbezpieczeństwa przez brak jednego ośrodka decyzyjnego, koordynującego działania innych instytucji publicznych. Wyzwań i problemów, przed którym stanął rząd było o wiele więcej. Niestety nie wszystkie z nich udało się rozwiązać.

Osiągniecia

Największym sukcesem jest z pewnością uchwalenie Ustawy o Krajowym Systemie Cyberbezpieczeństwa, która wdraża dyrektywę NIS do polskiego porządku prawnego. Opinie na temat nowego dokumentu są bardzo rozbieżne, przeważają jednak te krytyczne. Wśród zalet, najczęściej wymieniany jest fakt, że Ustawa w końcu powstała. Krytycy podkreślają też, że bez nacisku ze strony UE wciąż prawdopodobnie by jej nie było. Niezależnie od końcowej oceny tego dokumentu, w Polsce pojawiły się twarde zapisy prawne będące swoistym fundamentem do budowy systemu cyberbezpieczeństwa. Niestety Ustawa nie rozwiązuje głównego problemu, na który wskazywał NIK – odpowiedzialności instytucjonalnej za cyberbezpieczeństwo. W trakcie kadencji Minister Cyfryzacji Anny Streżyńskiej doszło do jej konfliktu z Ministrem Obrony Antonim Macierewiczem o to, kto powinien ponosić główną odpowiedzialność za cyberbezpieczeństwo w Polsce. Ustawa próbuje rozwiązać ten problem poprzez stworzenie stanowiska koordynatora ds. cyberbezpieczeństwa i kolegium ds. cyberbezpieczenstwa. Problem w tym, że nazwisko koordynatora powinno zostać ogłoszone do 28 listopada, a wciąż nie wiemy kim ta osoba będzie. Innym pytaniem jest jak ten system będzie funkcjonował w rzeczywistości. Na tę ocenę jest jeszcze za wcześniej.

Ważnym elementem było stworzenie Krajowych Ram Polityki Cyberbezpieczeństwa na lata 2017-2022. Dokument ten odgrywa rolę polskiej strategii cyberbezpieczeństwa i reprezentuje o wiele wyższy poziom jakościowy niż poprzednie koncepcje strategiczne. Nowa Ustawa sprawi jednak, że zostanie stworzony nowy dokument do 2019 roku. Czy jest sens co dwa lata pisać strategię czy może zamiast tego lepiej skupić się na realizacji jej zapisów?

To nie jedyne osiągniecia, które udało się zrealizować. Powołano też Narodowe Centrum

Cyberbezpieczeństwa (NC Cyber) w strukturze NASK, w którym gromadzone są informacje o zagrożeniach od różnych podmiotów biorących udział w przedsięwzięciu. Ważnym aspektem tej inicjatywy jest bliska współpraca z sektorem prywatnym i licznymi instytucjami takimi jak banki czy telekomy.

Warto również wspomnieć, że Ministerstwo Cyfryzacji zainteresowało się technologiami takimi jak blockchain czy AI, które stają się coraz ważniejsze. Na razie powstaje polska strategia AI i zobaczymy, czy uda się wdrożyć jej postanowienia czy po raz kolejny skończy się tylko na zapisach. Niestety w tym obszarze Polska jest lekko zapóźniona i musi gonić innych.

Problemy

Wciąż niedostateczne wydatki na cyberbezpieczeństwo stanowią jeden z głównych problemów Kwestia ta objawiła się już w trakcie konfliktu między Ministerstwem Cyfryzacji a Ministerstwem Obrony, kiedy ta pierwsza instytucja miał plany i koncepcje, ale niewielkie środki, natomiast MON o wiele większy budżet na ich realizację. Jak to powiedziała Minister Streżyńska nie można budować cyberbezpieczeństwa z grantów. Ustawa nie przynosi rozwiązania tego problemu, ponieważ sztywno planuje wydatki na następne 9 lat.

Kolejną rzeczą, która może wzbudzać niepokój jest rozwój polskiej armii w cyberprzestrzeni. NATO uznało środowisko wirtualne za kolejny obszar prowadzenia działań wojennych i członkowie powinni się do tego zastosować. W 2017 roku podczas forum CyberSec w Krakowie minister Antoni Macierewicz ogłosił utworzenie tzw. cyberarmii złożonej z 1000 osób. Po czym nastała cisza i do koncepcji tej wrócono podczas Komisji Obrony Narodowej na początku listopada. Paweł Dziuba, wicedyrektor Narodowego Centrum Kryptologii wspomniał, że prowadzone są “prace koncepcyjne nad powołaniem wojsk obrony cyberprzestrzeni“. Niestety widać, że rok został zmarnowany i pomysłu ministra Macierewicza nie wcielono i wciąż przeciągają się prace nad koncepcją.

Niestety pomimo wypowiedzi głównych decydentów na temat cyberbezpieczeństwa oraz ich udziału w ważnych branżowych konferencjach, jak np. premier Beata Szydło podczas Forum CyberSec w Krakowie, temat ten nie wciąż nie jest traktowany jako priorytetowy. Cyberataki nie kojarzą się z egzystencjonalnym zagrożeniem dla państwa i zbyt często są lekceważone i marginalizowane, gdzie priorytetem jest obrona przed konwencjonalną agresją. Prowadzi to do nieodpowiedzialnych pomysłów jak np. prób likwidacji Ministerstwa Cyfryzacji. Negatywnie przekłada się to również na państwowe wydatki na cyberbezpieczeństwo, które są niewystarczające. Problemy pojawią się również przy projektach cyfrowych realizowany przez Ministerstwo Cyfryzacji, nie są one wprost związane z cyberbezpieczeństwem, ale poruszają ważne kwestie. Opóźnienia we wdrożeniu programu CEPIK, awarie systemów rejestrów państwowych czy problemy z głosowaniem w wyborach samorządowych pokazują wiele problemów, przed którymi stoi Polska w zakresie cyfryzacji.

Podsumowując, plany w obszarze cyberbezpieczeństwa i cyfryzacji są i pozostają ambitne, ale często napotykają problemy administracyjne, finansowe czy po prostu brak zainteresowania głównych decydentów politycznych w kraju.