Cyberdefence 24

aut. Andrzej Kozłowski 14.10.2019

4 LATA PISU W CYBERPRZESTRZENI. CYBERBEZPIECZEŃSTWO DO POPRAWY [ANALIZA]

Cztery lata, które upłynęły od objęcia władzy przez PiS to czas niezwykle dynamicznych zmian w cyberprzestrzeni. To globalne epidemie WannaCry i NotPetya, zwiększona liczba ataków na infrastrukturę krytyczną czy zaawansowane operacje dezinformacyjne. Jak z tymi wyzwaniami poradził sobie polski rząd przez ostatnie 4 lata?

W połowie 2015 roku NIK opublikował raport, w którym niezwykle krytycznie oceniono stan polskiego cyberbezpieczeństwa. Ochrona bezpieczeństwa w cyberprzestrzeni nie była właściwa. Nie podjęto spójnych i systemowych działań w zakresie monitorowania i przeciwdziałania zagrożeniom występującym w cyberprzestrzeni. Aktywność państwa była paraliżowana przede wszystkim przez brak jednego ośrodka decyzyjnego, koordynującego działania innych instytucji publicznych oraz bierne oczekiwanie na rozwiązania, które w tym obszarze ma zaproponować Unia Europejska – charakteryzował cyberbezpieczeństwo w Polsce NIK w 2015 roku. Wykonany audyt w Ministerstwie Cyfryzacji doprowadził do odkrycia takich sytuacji, że np. CSIRT-y pracowały 8 godzinnie dziennie, a nie 24 godziny na dobę jak jest to powszechnie przyjętym standardem.

Sektor Cywilny

Ustawa o Krajowym Systemie Cyberbezpieczeństwa to z pewnością największe osiągnięcie, jeśli chodzi o cyberbezpieczeństwo ekipy rządowej. Wprowadza ona dyrektywę NIS do polskiego porządku prawnego, i sprawiła, że po raz pierwszy stworzono fundamenty do rozwoju systemu cyberbezpieczeństwa. Jakość tego dokumentu była jednak obiektem krytyki wielu ekspertów, którzy zarzucali, że jest to przejaw anachronicznego podejścia do problematyki cyberbezpieczeństwa. Nie sprecyzowano w nim również, kto faktycznie jest odpowiedzialny za realizację założeń w nim zawartych. Kontrowersje wzbudzały zbyt niskie środki przeznaczone na realizację założeń.

Argumentów przemawiających za zaletami wprowadzenia nowych rozwiązań nie było zbyt wiele i ograniczały się one do stwierdzeń, że dobrze, że w ogóle dokument powstał. Ustawa jedna funkcjonuje już rok a operatorzy usług kluczowych musieli, na jej mocy, wprowadzić odpowiednie narzędzia, co zwiększyło poziom cyberbezpieczeństwa. Istotne jest, że cyberbezpieczeństwo stało się w końcu tematem dyskusji polityków a nie tylko osób o technicznym wykształceniu. Obok Ustawy powstał również projekt Strategii Cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2019-2014, który wydaje się być poprawny i zwraca uwagę na najważniejsze kierunki strategiczne.

Rząd stoi jednak przed poważnymi wyzwaniami w obszarze cyberbezpieczeństwa. Jedno z nich to bardzo niski stopień bezpieczeństwa danych w samorządach – na co wskazał NIK w swoim raporcie. Zwracano uwagę na brak odpowiedniej świadomości zagrożenia wśród urzędników oraz systemowego podejścia. Podkreślono, że sytuacja nie uległa zmianie od poprzednich kontroli przeprowadzonych w 2014 i 2016 roku. Zmiany konieczne są jak najszybciej, a bez wsparcia rządu centralnego i dodatkowych funduszy będzie o nie trudno.

Dużo poważniejszym wyzwaniem jest bezpieczeństwo sieci 5G, czyli nowego standardu sieci telekomunikacyjnych, która umożliwi wprowadzanie na masową skalę Internetu rzeczy, Smart City czy autonomicznych samochodów. Obecnie toczy się dyskusja na poziomie europejskim i krajowym odnośnie bezpieczeństwa korzystania z rozwiązań niektórych producentów. Polski rząd się waha jaką decyzję powinien podjąć. Wydaje się, że czysto technologiczne względy schodzą na dalszy plan i zaczyna dominować polityka.

Walka z dezinformacją

Walka z fake newsami stała się jednym z najpopularniejszych haseł ostatnich lat. Należy jednak pamiętać, że to tylko narzędzie działań informacyjnych, które obejmują o wiele bardziej skomplikowane techniki. Niestety rząd nie ma pomysłu na przeciwdziałanie temu zjawisku. Po pierwsze nie radzi sobie na arenie międzynarodowej. Nie potrafi zbudować odpowiedniej narracji, która tłumaczyłaby nasze racje. Przykładem jest tutaj pozwolenie na kreowanie historii II wojny światowej przez Rosję, niemożność wykorzeniani ze świadomości sformułowania polskich obozów śmierci czy brak wyjaśnień, że demonizowana ustawa 447 uchwalona przez Kongres nie stanowi zagrożenia.

Problemy występują również na podwórku krajowym, gdzie liczne fake newsy wokół sieci 5G i wprowadzenie RODO zatruły debatę publiczną. Niestety brakuje skutecznej odpowiedzi. Ministerstwo cyfryzacji opublikowało raporty próbuję wyjaśnić te kwestie, ale nie odniosły one spodziewanego sukcesu. Innym problemem jest również bezpieczeństwo wyborów. Tutaj również stworzono raporty poświęcone dezinformacji oraz powołano do życia portal bezpiecznewybory.pl. Inicjatywy te choć potrzebne, są dalece niewystarczające. Raporty dotrą do niewielkiej liczby zainteresowanych, najczęściej ekspertów a portal bezpieczenwybory.pl jest mało znany szerokiemu gronu obywateli. Ponadto przypomina się o nim kilka tygodni przed wyborami, kiedy przez długi okres czasu pozostaje „martwy”. Warto pamiętać, że kampanie narracyjne trwają miesiącami a nawet latami, natomiast budowanie świadomości oraz wyposażanie obywateli w umiejętności odróżniania wiadomości prawdziwych od fałszywych to proces ciągły.

Sektor wojskowy

Również siły zbrojne zdynamizowały rozwój zdolności w cyberprzestrzeni. Ówczesny Minister Obrony Antonii Macierewicz w 2017 roku zadeklarował powołanie tysiąca „cyberżołnierzy”, którzy mieli w jego zamiarze odpowiadać za cyberbezpieczeństwo i walkę informacyjną. Na ten cel przeznaczono kwotę rzędu 2 miliardów złotych. Zwrócenie większej uwagi na problem cyberbezpieczeństwa było niejako pokłosiem decyzji podjętej na szczycie NATO w Warszawie w 2016 roku, gdzie uznano cyberprzestrzeń za kolejny obszar prowadzenia działań wojennych. Wraz ze zwiększającą się obecnością wojsk NATO na terytorium Polski, militarny aspekt cyberbezpieczeństwa musiał zostać uwzględniony. Dymisja ministra Macierewicza zastopowała ten proces, a koncepcja cyberwojsk została odłożona w czasie i powrócono do niej dopiero w 2019 roku. Zapowiedziano stworzenie dowództwa wojsk do 2022 roku, a osiągnięcie zdolności operacyjnej do 2024 roku. Późno? Oczywiście, że tak, ale można powiedzieć, że lepiej późno niż wcale. Niestety koncepcja cyberwojsk nie została upubliczniona, więc ciężko jest dyskutować o szczegółach. Z dostępnych informacji wynika, że wojsko ma zamiar centralizować zasoby odpowiedzialne za cyberbezpieczeństwo, co jest dobrym pomysłem, chociażby ze względu na niewielkie zasoby sił zbrojnych. Drugim dobrym pomysłem, jest podstawienie na edukację młodzieży poprzez m.in stworzenie Wojskowego Liceum Informatycznego oraz większe otwarcie się na ekspertów zewnętrznych. Ma to rozwiązać jeden z problemów, czyli brak odpowiedniej ilości specjalistów. Kolejny pomysł MON-u, czyli podstawienie na komponent cyber w Wojskach Obrony Terytorialnej, ma taki sam cel. Wzorując się tutaj na rozwiązaniach amerykańskiej Gwardii Narodowej, wojsko chce zachęcić cywilnych ekspertów ds. cyberbezpieczeństwa do większego zaangażowania się w ramach WOT-u. Pomysł ten należy ocenić jako dobry, który sprawdził się w USA. Pierwsze reakcje w

Polsce też są pozytywne. Niestety wciąż nie wiadomo, jak wojsko podchodzi do operacji ofensywnych w cyberprzestrzeni, współpracy z sektorem cywilnym czy komponentu „infoops". Warto było wyjaśnić opinii publicznej te zagadnienia.

Wnioski

Poseł PiS Jacek Sasin powiedział, że Polska za czasów PiS stała się bezpieczna w cyberprzestrzeni. Oczywiście jest to stwierdzenie nieprawdziwe, która pokazuje niską świadomość polityków w obszarze bezpieczeństwa teleinformatycznego. Z pewnością jednak przez ostatnie 4 lata działania w obszarze cyberbezpieczeństwa uległy zdynamizowaniu. Wiele rzeczy można było zrobić lepiej, ale ważne, że zbudowano fundamenty pod dalszy rozwój.

W przyszłości, cyfryzacja i cyberbezpieczeństwo będą tylko ważniejsze, dlatego konieczne będzie przeznaczenie większej liczby pieniędzy na ten cel i uczynienie go jednym z priorytetów. W innym wypadku, znowu świat odjedzie Polsce, a ta nie będzie w stanie go już dogonić.