aut. Andrzej Kozłowski 14.08.2019

NOWA STRATEGIA CYBERBEZPIECZEŃSTWA KROKIEM W DOBRĄ STRONĘ [ANALIZA]

Ministerstwo Cyfryzacji opublikowało projekt Strategii Cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2019-2024. Nowy dokument jest prawidłowo sformułowaną strategią, która jasno precyzuje najważniejsze cele Polski w cyberprzestrzeni. Porusza również najważniejsze elementy cyberbezpieczeństwa dla współczesnego państwa. Nie odstaje od innych strategii cyberbezpieczeństwa państw Unii Europejskiej.

Nowy dokument jest bazuje podobny do stworzonych niedawno Ram Polityki Cyberbezpieczeństwa na lata 2017-2022 i stanowi jego rozwinięcie. Jest to słuszna koncepcja, ponieważ tworzenie zupełnie różnych strategicznych dokumentów w krótkim okresie mija się z celem. Oba akty nieznacznie się od siebie różnią i warto przeanalizować główne zmiany, które nastąpiły.

Nowa Strategia za główny cel obiera uzyskanie wysokiego poziomu cyberbezpieczeństwa rozumianego jako odporność systemów najważniejszych podmiotów państwowych. Pytanie jak zostanie to ocenione. Czy Ministerstwo ma przyjętą jakąkolwiek metodologię pozwalającą na ocenę poziomu cyberbezpieczeństwa poszczególnych instytucji i jego zmianę w czasie?

W dokumencie podkreśla się, że jednym z kluczowych elementów będzie standaryzacja zabezpieczeń oraz wzmacnianie Krajowego Systemu Cyberbezpieczeństwa (KSC) co jest głównym nowym elementem w porównaniu do Krajowych Ram. W momencie ich tworzenia nie było jeszcze KSC. Projekt strategii podobnie jak Krajowe Ramy podkreślają związek i znaczenie cyberbezpieczeństwa dla bezpieczeństwa narodowego oraz przywiązanie do wolnego i otwartego Internetu. W projekcie strategii brakuje jednak jasnego określenia zasobów, które Polska posiada do realizacji jej celów strategii oraz przedstawienia zagrożeń w wymiarze strategicznym dla kraju w cyberprzestrzeni. Autorzy nie przedstawiają jasno, jakie mogą być skutki zaniedbań cyberbezpieczeństwa w kraju.

W projekcie strategii wymieniono następujące cele szczegółowe:

- Rozwój Krajowego Systemu Cyberbezpieczeństwa;
- Podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania incydentom;
- Zwiększenie potencjału narodowego w zakresie technologii cyberbezpieczeństwa;
- Budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa;
- Zbudowanie silnej pozycji międzynarodowej Polski w obszarze cyberbezpieczeństwa.

Projekt strategii zakłada, że podstawą rozwoju KSC jest dokonanie pełnego wdrożenia i oceny funkcjonowania przepisów ustanawiających ten system. Strategia wskazuje na działania, które mają zostać podjęte, aby podnieść efektywne działanie tego systemu w przyszłości. Do zadań tych należy m.in. uruchomienie systemu teleinformatycznego do roku 2021 który będzie wspierał:

- Współpracę podmiotów wchodzących w skład KSC;
- Generowanie i przekazywanie rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa;
- Zgłaszanie i obsługę incydentów;
- Szacowanie ryzyka na poziomie krajowym;
- Ostrzeganie o zagrożeniach cyberbezpieczeństwa.

W projekcie strategii zapowiedziano również rozwój CSIRTów poziomu krajowego oraz poprawienie współpracy pomiędzy nimi poprzez wdrożenie systemowych rozwiązań. Jest to ciekawe, o jakich systemowych rozwiązań mowa, bo takim rozwiązaniem powinna być ustawa o KSC. Twórcom strategii należy się pochwała za zwrócenie uwagi na problem bezpieczeństwa jednostek samorządu terytorialnego (JST). Poziom cyberbezpieczeństwa samorządów dotychczas oceniany był na bardzo niskim poziomie, co wykazała ostania kontrola NIKu. Bez wsparcia ze strony władz rządowych nie będą one w stanie odpowiednio zabezpieczyć swoich systemów i sieci teleinformatycznych oraz co najważniejsze, danych obywateli.

Kolejnym ważnym elementem poprawiającym funkcjonowanie KSC ma być zgodnie z zapisami dokumentu wprowadzenie przez administrację publiczną obowiązkowej standaryzacji i minimalnych wymagań cyberbezpieczeństwa w ramach Narodowych Standardów Cyberbezpieczeństwa. Autorzy strategii mają nadzieję, że będzie to wyznacznik również dla sektora prywatnego oraz dla obywateli. Jak na razie niewiele wiadomo o procesie standaryzacji. Z pewnością będzie ona wykorzystywała unijne ramy standaryzacji, ale warto również zapytać czy będzie się to wiązało z gruntowanym audytem w jednostkach administracji publicznej i wymianą sprzętu, czy znajdą się na to fundusze i kto miałby przeprowadzić takie działania.

Dobrym pomysłem zawartym w projekcie jest weryfikacja efektywności funkcjonowania KSC przez ćwiczenia krajowe oraz ćwiczenia sektorowe. Wciąż jednak nie wiadomo więcej na temat tych inicjatyw. Czy ćwiczenia będą tylko techniczne przeznaczone dla osób związanych z techniczną obsługa systemu, czy może również będą miały miejsce na poziomie strategicznym dla decydentów politycznych, urzędników i samorządowców? Strategia nie zawiera również informacji w jakim okresie czasu będą przeprowadzane.

Projekt Strategii zakłada również, rozbudowę systemu wymiany informacji zarówno na poziomie strategicznym i operacyjnym. Ale również pomiędzy sektorem cywilnym i wojskowym. Brakuje jednak konkretnych pomysłów, w jaki sposób to zrealizować. Sytuacja podobnie wygląda w przypadku wspierania partnerstwa publiczno-prywatnego. Nie zaprezentowano żadnych konkretnych inicjatyw.

Rząd obiecuje również wsparcie cyberbezpieczeństwa operatorów infrastruktury krytycznej, podkreślając jej znaczenie dla bezpieczeństwa państwa. Proponowane jest tutaj ustalenie minimalnych wymagań w zakresie cyberbezpieczeństwa ze szczególnym uwzględnieniem zarządzania ciągłością działania. Co ciekawe, analogicznym reżimem mają być również objęci dostawcy usług cyfrowych. Kluczowa w realizacji tego pomysłu ma być współpraca w ramach Grupy Współpracy Dyrektywy NIS, a także z podmiotami brytyjskimi i amerykańskimi. Pomóc w zabezpieczeniu infrastruktury krytycznej może również wprowadzenie jednolitej metodyki szacowania ryzyka na poziomie krajowym, która uwzględnia specyfikę poszczególnych sektorów, co zostało ogłoszone w strategii. Ma być to proces ciągły. Metodyka powstaje w ramach Narodowej Platformy Cyberbezpieczeństwa, która jest finansowana przez Narodowe Centrum Badań i Rozwoju.

W ramach drugiego celu szczegółowego zwraca się szczególną uwagę na bezpieczeństwo łańcucha dostaw, gdzie zamierza się utworzyć krajowy system oceny i certyfikacji oraz przeprowadzać testy i audyty cyberbezpieczeństwa, w tym również poprzez programy Bug-Bounty, czyli takie w których poszukiwanie podatności zaangażowane są osoby niezwiązane z producentem tego oprogramowania.

Na całym świecie są one ocenianie pozytywnie i jest to dobry sygnał, że administracja uwzględniła to rozwiązanie. Eksperci od dawna rekomendowali skorzystanie z takich programów.

Strategia porusza również kwestie militarne informując, że Polska musi posiadać zdolność prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni, w tym operacji ofensywnych, rozumianych w dokumencie jako zwalczanie źródeł zagrożeń.

Dokument zakłada również wykorzystanie polskich zasobów przemysłowych i technologicznych. Projekt strategii mówi o rządowym wsparciu dla polskiego biznesu, które ma się wyrażać m.in. poprzez pomoc państwa dla firm ubiegających się o środki na rozwój innowacyjnych rozwiązań. Zapowiadane jest tworzenie sprzyjających warunków do rozwoju start-upów, których przedmiotem miałoby być wytwarzanie nowoczesnych rozwiązań w obszarze bezpieczeństwa. Dokument zakłada również współpracę międzynarodową i udział w planowym Europejskim Centrum Kompetencji Cyberbezpieczeństwa. Projekt strategii przewiduje także zwiększenie na uczelniach wyższych liczby studentów i naukowców zajmujących się cyberbezpieczeństwem. Warto jednak zastanowić się jak ma on funkcjonować w realiach polskiego świata naukowego. Autorzy strategii upatrują tutaj szansę w programach badawczych Narodowego Centrum Badań i Rozwoju, międzynarodowych projektach badawczych oraz organizacjach pozarządowych. Dokument zapowiada również promowanie idei security by design na etapie projektowania technologii, w szczególności w kontekście Internetu rzeczy.

Bardzo ważnym elementem każdej strategii jest wkomponowanie społeczeństwa w budowę systemu cyberbezpieczeństwa. Zapowiadane są różnego rodzaju programy, ukierunkowane na podniesienie poziomu edukacji na wszystkich szczeblach, od wczesnoszkolnej do akademickiej oraz doskonalenia zawodowego. Należy jednak zapytać czy te poważne zmiany w systemie edukacji były konsultowane z Ministerstwem Edukacji i jak zostaną wdrożone do systemu nauczania na różnych szczeblach. Ważnym elementem jest również organizowanie kampanii społecznych, które uwrażliwiają ludzi na zagrożenia w świecie cyfrowym, w tym również na dezinformację i propagandę. Cel sam w sobie jest bardzo dobry, tylko, że należałoby zadać pytać o skuteczność podejmowanych wcześniej działań. Dotychczas prowadzone kampanie edukacyjne nie przyniosły pożądanych rezultatów.

Strategia stawia sobie też bardzo ambitny cel, czyli zbliżenia zarobków członków administracji publicznej o wysokich kompetencjach do poziomu, który mogliby uzyskać w sektorze prywatnym. Strategia nie wspomina jednak o jakiego szczebla pracowników chodzi oraz jakiej branży. Jest to bardzo ambitne zadanie, a problem z pozyskaniem osób do pracy w sektorze IT w administracji państwowej mają wszystkie kraje.

Ostatnia część projektu strategii dotyczy współpracy międzynarodowej i jest praktycznie identyczna z tym, co zostało zawarte w Ramach Polityki Cyberbezpieczeństwa. Na arenie międzynarodowej stawia się na współpracę z Unią Europejską, NATO, ONZ oraz kooperacje w regionie w ramach Grupy Wyszehradzkiej i Trójmorza. Podkreśla się międzynarodową współpracę zarówno na poziomie operacyjnym jak i strategicznym. W dzisiejszym świecie cyberbezpieczeństwo stało się nieodłącznym elementem polityki, dlatego Polska musi aktywnie brać udział w dyskusjach na ten temat na forum międzynarodowym. W szczególności, że geopolityka świata technologicznego zmienia się i być może w niedalekiej przyszłości dojdzie do fragmentaryzacji cyberprzestrzeni na Wschód i Zachód.

Wraz z wejściem nowej Strategii w życie, a ma to się stać do 31 października, przestaną obowiązywać Krajowe ramy Polityki Cyberbezpieczeństwa na lata 2017-2022. Nowa strategia zostanie wdrożona ze względu na wymagania dyrektywy NIS, która tą dyrektywę przenosi, na mocy ustawy o KSC, na grunt polski. Nowy dokument zostanie uchwalony na okres 5 lat, a koordynatorem wdrażania jest Minister cyfryzacji. Jest to dobra wiadomość, ponieważ w końcu na kimś spoczywa konkretna odpowiedzialność i kogo można rozliczyć za ewentualne nieprawidłowości. Zaplanowano również dwa przeglądy

dokumentu, odpowiednio po 2 i 4 latach. W projekcie zapowiedziano również publikację w przeciągu 6 miesięcy Planu działań na rzecz wdrożenia Strategii Cyberbezpieczeństwa, w którym to zostaną przedstawione już konkretne inicjatywy oraz oszacowane koszty finansowania. Opublikowanie Planu pozwoli również na łatwiejszą ocenę rzeczy, które zostały wykonane w celu poprawy cyberbezpieczeństwa.

Strategia jest dokumentem prawidłowo sformułowanym, zmieniającym niektóre aspekty Ram Polityki Cyberbezpieczeństwa, ale zachowującym jej główne idee i priorytety. Porusza najważniejsze elementy cyberbezpieczeństwa dla współczesnego państwa. Nie odstaje od innych strategii państw Unii Europejskiej. Teraz przyjdzie moment na zrealizowanie jej założeń, co będzie wymagało o wiele większego wysiłku i pieniędzy oraz pozwoli uniknąć polskiej bolączki - masowej produkcji dokumentów strategicznych, które nie są wdrażane w życie.