Cyberdefence 24

aut. Andrzej Kozłowski 30.09.2016

STRATEGIA CYBERBEZPIECZEŃSTWA RP - "CYFROWY" PRZEŁOM W DZIAŁANIACH POLSKI [KOMENTARZ]

Ministerstwo Cyfryzacji przedstawiło dzisiaj projekt uchwały w sprawie Strategii Cyberbezpieczeństwa RP na lata 2016 – 2020. Dokument, na który czekało wielu ekspertów od cyberbezpieczeństwa, jest dobrą strategią i stanowi fundament pod dalszy rozwój systemu cyberbezpieczeństwa. Jakościowo zdecydowanie przewyższa osiągnięcia poprzedników.

Warto przyjrzeć się najważniejszym postanowieniom tego liczącego 28 strony dokumentu. Na wstępie definiuje on czym jest akceptowalny poziom bezpieczeństwa. Termin ten jest rozumiany jako: zapewnienie zdolności do realizacji funkcji Państwa, zapewnienie ludności i przedsiębiorstwom dostaw towarów i usług oraz niezakłóconego dostępu i korzystania z sieci Internet.

Realizacja tych celów ma zostać zapewniona poprzez stworzenie ram organizacyjno-prawnych oraz skutecznej koordynacji i wymiany informacji pomiędzy użytkownikami tego systemu.

Wydaje się, że cele szczegółowe strategii zostały poprawnie zdefiniowane i uwzględniają najważniejsze obecnie obszary polityki cyberbezpieczeństwa. Wśród 7 najważniejszych znalazło się:

1. zwiększenie poziomu bezpieczeństwa infrastruktury teleinformatycznej państw,
2. zwiększenie zdolności do zapobiegania i zwalczania zagrożeń ze strony cyberprzestrzeni,
3. zmniejszenie skutków incydentów godzących w bezpieczeństwo cyberprzestrzeni,
4. określenie kompetencji podmiotów odpowiedzialnych za bezpieczeństwo cyberprzestrzeni,
5. stworzenie spójnego systemu zarządzania bezpieczeństwem w cyberprzestrzeni,
6. stworzenie trwałego systemu koordynacji i wymiany informacji między podmiotami odpowiedzialnym za bezpieczeństwo w cyberprzestrzeni,
7. zwiększenie świadomości użytkowników w zakresie metod i środków bezpieczeństwa,

Do wymienionych celów można byłoby dodać zabezpieczenie łańcucha dostaw sprzętu i oprogramowania oraz utworzenie odpowiednich regulacji prawnych.

Ważnym elementem strategii jest podział na użytkowników internetu, gdzie wyróżniono obywateli, przedsiębiorców, pracowników administracji publicznej, oraz operatorów usług kluczowych. Szczególnie ważne jest uczynienie z wszystkich internautów pierwszej linii obrony, dzięki odpowiedniej świadomości zagrożeń wśród nich. Pozwoli to na zdecydowane zmniejszenie liczby incydentów w środowisku wirtualnym.

Po raz pierwszy w strategii pojawił się wymiar międzynarodowy polityki cyberbezpieczeństwa, gdzie zdefiniowano najważniejsze założenia i cele Polski w tym obszarze oraz przedstawiono pogląd na kwestię wolności w Internecie.

Stanowisko rządu nie odbiega tutaj od wizji Unii Europejskiej, Stanów Zjednoczonych czy innych krajów należących do państw zachodnich. Zapowiedziano również większą aktywności dyplomacji polskiej na forach organizacji międzynarodowych zajmujących się tą problematyką. Cieszy również podkreślenie znaczenia Ministerstwa Spraw Zagranicznych w tym obszarze, o czym mówi się po raz pierwszy.

Strategia wymienia trzy wymiary działań: strategiczny, operacyjny, techniczny. Na poziomie strategicznym mają dominować działania o charakterze zarządczym - wymieniono tutaj zadania głównych instytucji, takich jak Biuro Bezpieczeństwa Narodowego, Ministerstwo Sprawiedliwości, Agencja Bezpieczeństwa Wewnętrznego, Ministerstwo Obrony Narodowej, Ministerstwo Spraw Wewnętrznych i Administracji, Komendant Główny Policji oraz Ministerstwo Cyfryzacji.

Na poziomie operacyjnym mają być prowadzone działania mające na celu zapobieganie, wykrywanie, przeciwdziałanie w odniesieniu do potencjalnych ataków oraz reagowanie na rozwijający się atak. Konieczny jest tutaj efektywny system zarządzania ryzykiem, dlatego strategia ma zamiar wprowadzić jednolitą metodykę szacowania ryzyka oraz sprawną wymianę informacji. Poziom techniczny to domena aktywności właścicieli sieci systemów teleinformatycznych. Podział na poziomy wydaje się być pożądany, ale pojawia się pytanie jednak jak będzie przebiegała współpraca i interakcja pomiędzy podmiotami odpowiedzialnym za każdy z tych obszarów?

System polskiego cyberbezpieczeństwa będzie składał się z trzypoziomowego systemu ochrony cyberprzestrzeni i obejmował ochronę nie tylko instytucji państwowych, ale również sektora prywatnego i obywateli. Słusznie zauważono, że mogą oni zainfekować swoje urządzenia złośliwym oprogramowaniem i tym samym stwarzać zagrożenie dla systemów państwowych. W skład systemu wejdzie minister właściwy do spraw informatyzacji, jako rządowy organ koordynujący na poziomie polityczno-strategicznym, właściwi ministrowie - zgodnie z zakresami kompetencji, NCCyber, CSIRT sektorowe oraz kierownicy urzędów i instytucji. Przy powołaniu Ministra właściwego ds. informatyzacji należałoby wziąć pod uwagę doświadczenia innych państw z podobnymi stanowiskami. Dobrym przykładem są tutaj Stany Zjednoczone, gdzie jedna osoba odpowiedzialna za koordynację polityki cyberbezpieczeństwa miała duże problemy z wypełnieniem swoich zadań.

W ramach administracji publicznej przewiduje się stworzenie klastrów bezpieczeństwa, które obejmą administrację rządową oraz samorządową. Zostaną one zbudowane w celu zapewnienia dodatkowej ochrony danych, która ma polegać na bezpośredniej ochrony danych oraz budowy architektury zwiększającej to bezpieczeństwo.

W ramach bezpieczeństwa informacji zostanie powołany w każdej instytucji kierownik jednostki, który ustanowi system zarządzania bezpieczeństwem informacji - co miejmy nadzieję uchronić nas przed wyciekami danych, takich jak tzw. akta Snowdena.

Strategia zwraca baczną uwagę na świadomość społeczeństwa oraz stworzenie wykwalifikowanych kadr. Rekomenduje się edukację w zakresie cyberbezpieczeństwa od szkoły podstawowej, ale również uświadamianie osób starszych poprzez kampanię informacyjną, co jest bardzo dobrym pomysłem. Zakłada się również szkolenia dla pracowników organów ścigania i administracji publicznej, co jest absolutnie konieczne. Pytaniem pozostaje ich jakość i sposób sprawdzenia wykorzystania zdobytych informacji w praktyce.

Niezwykle istotny jest fakt, że strategia podkreśla konieczność współpracy z ośrodkami akademicki poprzez stworzenie Naukowego Akademickiego Klastra Cyberbezpieczeństwa podnoszącego kompetencje ośrodków naukowych w obszarze cyberbezpieczeństwa. Przewiduje się również intensyfikację współpracy pomiędzy sektorem publicznym i prywatnym poprzez stworzenie forum dialogu pomiędzy tymi sektorami w ramach Forum ds. Cyberbezpieczeństwa.

Osiągnięcie celów Strategii będzie wymagało zorganizowania krajowego systemu cyberbezpieczeństwa z podmiotami prywatnymi i państwowymi, koordynacją krajowych działań z wysiłkami międzynarodowymi oraz współpracy z ośrodkami akademickim, sektorem prywatnym oraz organizacjami pozarządowymi.

Elementy brakujące

Strategia pomija jednak niektóre z ważnych aspektów. Brakuje tutaj stworzenia mapy zagrożeń przedstawiającej jakie są najpoważniejsze wyzwania i określeniem prawdopodobieństwo ich wystąpienia. Można byłoby to dodać na końcu artykułu wzorując się na strategii Austrii. Szczególnie martwi zignorowanie zagrożeń insiderskich, które - jak pokazują ostatnie wydarzenia na świecie - stanowią coraz większe wyzywanie.

Kolejnym elementem, który mógłby się znaleźć w strategii, to precyzyjne przedstawienie zadań do realizacji w konkretnym obszarze czasu, jak miało to miejsce w strategii cyberbezpieczeństwa Wielkiej Brytanii.

Zabrakło również odniesienia do kwestii etycznych, szczególnie biorąc pod uwagę fakt, że temat niedoboru kadr oraz edukacji został w dokumencie mocno zaakcentowany.

Ponadto, pomimo odniesienia się do nowoczesnych technologii jak np. internetu rzeczy czy Smart City, zabrakło tematu chmury obliczeniowej i sposobu wykorzystania jej przez rząd.

Podsumowując, strategia wydaje się być dobrym fundamentem do dalszych prac nad polityką cyberbezpieczeństwa RP. Wprowadza ona podstawowe rzeczy, które powinny zostać zrealizowane już dawno. W szczególności cieszy podkreślenie aspektu edukacyjnego oraz znaczenia świadomego zagrożenia obywatela jako pierwszej linii obrony. Wprawdzie strategia ma pewne braki, które zostały wymienione powyżej, ale można je uzupełnić w toku dalszych prac. Bardzo ważny będzie proces wdrażania tych ambitnych rozwiązań oraz kształt i treść Ustawy o cyberbezpieczeństwie. Strategia wyznacza tylko pewne kierunki i definiuje główne cele, które trzeba następnie zrealizować w praktyce i w wielu miejscach uszczegółowić. Od jakości tych prac będzie zależała jakość polskiego sytemu cyberbezpieczeństwa.

Czytaj też: Resort cyfryzacji ujawnia polską Strategię Cyberbezpieczeństwa