Współpraca międzysektorowa szansą na bezpieczeństwo cyfrowe

W Ministerstwie Cyfryzacji powstaje właśnie „Strategia cyberbezpieczeństwa Rzeczpospolitej Polskiej". Zgodnie z zapisami Strategii „rozwój społeczny i gospodarczy w coraz większym stopniu zależny jest od szybkiego i nieskrępowanego dostępu do informacji oraz jej wykorzystania w zarządzaniu, produkcji, sektorze usług oraz przez podmioty publiczne. Stały rozwój sieci i systemów informatycznych, w tym operacje na dużych zasobach danych, służą rozwojowi komunikacji, handlu, transportu czy też usług finansowych. W cyberprzestrzeni tworzymy i kształtujemy relacje społeczne, a Internet stał się narzędziem do wpływania na zachowania grup społecznych, a także oddziaływania w sferze politycznej". Wobec strategicznego znaczenia owego obszaru konieczne jest zapewnienie odpowiednich warunków działania dla wszystkich podmiotów tworzących krajowy system cyberbezpieczeństwa, a więc podmiotów gospodarczych świadczących usługi przy wykorzystaniu systemów teleinformatycznych, użytkowników cyberprzestrzeni, organów władzy publicznej, a także wyspecjalizowanych podmiotów zajmujących się bezpieczeństwem teleinformatycznym w sferze operacyjnej.

Celem Strategii jest określenie ramowych działań, mających na celu uzyskanie wysokiego poziomu odporności krajowych systemów teleinformatycznych, operatorów usług kluczowych, operatorów infrastruktury krytycznej, dostawców usług cyfrowych oraz administracji publicznej na incydenty w cyberprzestrzeni. Proponowane kierunki strategiczne mają również wpływać na zwiększenie skuteczności organów ścigania i wymiaru sprawiedliwości w wykrywaniu i zwalczaniu przestępstw oraz działań o charakterze terrorystycznym i szpiegowskim w cyberprzestrzeni. Strategia jest spójna z prowadzonymi działaniami dotyczącymi operatorów infrastruktury krytycznej wykorzystujących systemy teleinformatyczne oraz uwzględnia potrzeby zaangażowania Sił Zbrojnych Rzeczypospolitej Polskiej.

Swoje zadania w zakresie cyberbezpieczeństwa realizować muszą również samorządy, jako administracja publiczna zarządzająca szeroką gamą usług publicznych, jak i nadzorujące liczne jednostki organizacyjne zaliczane do operatorów infrastruktury krytycznej, jak np. systemy wodno-kanalizacyjne czy Szpitalne Odziały Ratunkowe. Niestety, jak każdy obszar działań publicznych, również cyberbezpieczeństwo wymaga zaangażowania odpowiednich zasobów ludzkich, finansowych i organizacyjnych. W naturalny sposób rodzi się więc pytanie: **w jaki sposób sektor prywatny może włączyć się w działania publiczne w obszarze cyberbezpieczeństwa?**

Przygotowywana w Ministerstwie Strategia dotycząca cyberbezpieczeństwa odnosi się również do budowania mechanizmów współpracy między sektorem publicznym i prywatnym[1]. Zgodnie z założeniami przywołanego dokumentu „Zapewnienie bezpieczeństwa w cyberprzestrzeni wymaga wspólnego wysiłku sektora prywatnego, publicznego oraz obywateli. Rząd będzie dążył do zbudowania efektywnego systemu partnerstwa publiczno-prywatnego opartego na zaufaniu i wspólnej odpowiedzialności za bezpieczeństwo w cyberprzestrzeni. Jednocześnie, administracja publiczna będzie doskonaliła swój potencjał w zakresie doradzania sektorom rynkowym w dziedzinie bezpieczeństwa teleinformatycznego. Rząd będzie również aktywnie angażować się w istniejące i powstające formy europejskiej współpracy publiczno-prywatnej i tym samym promować polski biznes na arenie międzynarodowej. Realizując nową wizję rozwoju kraju i wspierając innowacyjność polskiej gospodarki, istotna będzie budowa systemu wsparcia przedsięwzięć badawczo-rozwojowych w dziedzinie cyberbezpieczeństwa, w tym projektów realizowanych we współpracy ze światem nauki oraz z przedsiębiorstwami komercyjnymi".

Wobec realizacji pierwszych projektów w zakresie rozwoju sieci teleinformatycznej prowadzonych w modelu PPP, Forum PPP postanowiło przybliżyć czytelnikom, w jakim zakresie sektor prywatny, administracja centralna i samorządowa mogą współpracować w obszarze cyberbezpieczeństwa. **Wszystkich przedstawicieli administracji publicznej, rozważających współpracę w zakresie wspólnego udzielania zamówień publicznych w obszarze cyberbezpieczeństwa, zainteresować powinna możliwość wsparcia ze strony Ministerstwa Cyfryzacji w ewentualnym przygotowaniu wspólnego zamówienia. Na kolejnych stronach przedstawiamy Państwu rozmowę z Karolem Okońskim, Sekretarzem Stanu, Pełnomocnikiem Rządu do spraw Cyberbezpieczeństwa w Ministerstwie Cyfryzacji**.

Bartosz Korbus

[1] Por. pkt 7.2 projektu Strategii – dostęp: https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022