

Quantum Cybersecurity Group wspomaga jednostki samorządu terytorialnego w uzyskaniu finansowania dla samorządów pt.

„Cyberbezpieczny samorząd”

Projekt grantowy „Cyberbezpieczny samorząd” jest realizowany w odpowiedzi na potrzeby jednostek samorządu terytorialnego, wykryte w ramach „Diagnozy cyberbezpieczeństwa”.

Badanie to wykazało, że „u dużego odsetka JST występują nawet problemy ze spełnieniem minimalnych wymogów bezpieczeństwa zdefiniowanych w obowiązujących przepisach prawa”. Stąd, na podstawie RODO, uoKSC i KRI, opracowano dla JST propozycję 4-fazowej ścieżki rozwoju z zakresu cyberbezpieczeństwa (Rysunek 1). Analogicznie do niej, Quantum Cybersecurity Group przygotowało ofertę 4-fazowego projektu weryfikacji i ew. podniesienia poziomu cyberbezpieczeństwa JST.

W celu realizacji proponowanego projektu QCG oferuje bezpłatną usługę przygotowania i złożenia aplikacji grantowej o fundusze z projektu „Cyberbezpieczny samorząd” w imieniu JST.

Następnie zespół ekspertów przeprowadzi audyt cyberbezpieczeństwa (realizacja KRI §20 ust. 2 pkt. 4) oraz szereg szkoleń specjalistycznych (realizacja KRI §20 ust. 2 pkt. 6), zwłaszcza z zakresu nowych zagrożeń ze strony komputerów kwantowych.

W oparciu na wynikach audytu, QCG przeprowadzi konsultacje z kluczowym personelem JST w celu

W przeciągu pięciu do dziesięciu lat komputery kwantowe złamią dziś nam znane metody szyfrowania.”

Sundar Pichai, CEO Google (World Economic Forum 2020, [link](#))

zaplanowania działań potrzebnych do uzupełnienia, utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji (realizacja KRI §20 ust. 1). Kolejne kroki, wchodzące w obszar działań i implementacji, obejmować mogą m.in.:

... Wdrożenie polityki uprawnień i wdrożenie nowoczesnych systemów uwierzytelniania i weryfikacji z wykorzystaniem algorytmów post-kwantowych oraz kwantowo generowanych liczb losowych (realizacja KRI §20 ust. 2 pkt. 4 i 5);

... Wprowadzenie zabezpieczeń sieci, w tym urządzeń mobilnych, w postaci adekwatnych procedur oraz korzystania z szyfrowania algorytmami post-kwantowymi z wykorzystaniem kwantowo generowanych liczb losowych (realizacja KRI §20 ust. 2 pkt. 7c, 8 i 9);

... Zabezpieczenie plików i danych za pomocą szyfrowania przy użyciu algorytmów post-kwantowych z wykorzystaniem generowanych kwantowo liczb losowych (realizacja KRI §20 ust. 2 pkt. 12D i 12E);

... Regularną obsługę wdrożonych rozwiązań, podnoszenie kompetencji oraz kontrolę systemu zarządzania bezpieczeństwem informacji.

Poza rozwiązaniami klasycznymi, oferowanymi również przez inne firmy, QCG wyróżnia się na rynku zastosowaniem technologii kwantowych w cyberbezpieczeństwie, w odpowiedzi na rosnące zagrożenie ze strony komputerów kwantowych. Urządzenia kryptograficzne QCG są gotowe do natychmiastowego użycia zaraz po instalacji w obecnych systemach IT bez wymogu zmiany ich struktury, w myśl podejścia „plug & play”.

Wnioski o dofinansowanie można składać do **13 października** b.r. Środki można przeznaczyć na wydatki w obszarach:

1. Organizacyjnym – audyty, aktualizacje & wdrażanie Polityki Bezpieczeństwa Informacji (PBI) oraz Systemu Zarządzania Bezpieczeństwem Informacji (SZBI);
2. Kompetencyjnym – szkolenia;
3. Technicznym – zakup, wdrożenie i utrzymanie systemów teleinformatycznych, ciągłego monitorowania bezpieczeństwa, urządzeń, usług, wsparcia, badań i testów.