Magiczny Kraków

Kraków zyskuje przewagę w cyberbezpieczeństwie

2026-01-09

Dzięki wdrożeniu przez Akademickie Centrum Komputerowe Cyfronet AGH technologii kwantowej dystrybucji klucza, Urząd Miasta Krakowa stał się pierwszą instytucją połączoną w ten sposób z centrum obliczeniowym. To przełomowy krok, który otwiera nową erę bezpiecznej komunikacji i wzmacnia rolę Krakowa jako miasta stawiającego na najdoskonalsze, bo kwantowe, rozwiązania w zakresie cyberbezpieczeństwa.

Kwantowa tarcza ochronna na rzecz Krakowa

Technologia kwantowej dystrybucji kluczy szyfrujących (zwana dalej QKD – *Quantum Key Distribution*) to jedna z najnowocześniejszych technologii kryptograficznych. Wykorzystuje prawa mechaniki kwantowej, by tworzyć i przesyłać klucze szyfrujące. Jej wyjątkowość polega na tym, że każda próba przechwycenia transmisji automatycznie niszczy klucz i uruchamia alarm. Klucze są generowane w czasie rzeczywistym, co eliminuje potrzebę ich przechowywania i zapewnia maksymalny poziom ochrony. Specjaliści z ACK Cyfronet AGH zaprojektowali, zbudowali i uruchomili system kwantowej dystrybucji kluczy szyfrujących pomiędzy Urzędem Miasta Krakowa a Cyfronetem AGH. Jest to pierwsze w regionie tego typu połączenie, które umożliwia przesyłanie kluczy szyfrujących, wykorzystywanych do zabezpieczania łącza sieciowego o przepustowości 100 Gbps (gigabitów na sekundę).

– Dzięki temu możliwe jest bezpieczne przesyłanie danych między instytucjami, m.in. w celu archiwizacji, wymiany baz danych, analizy danych czy wzbogacania treści serwisów informacyjnych Urzędu Miasta Krakowa – wyjaśnia Karol Krawentek, zastępca dyrektora ACK Cyfronet AGH ds. Infrastruktury Centrum Danych.

Cyfrowa Tarcza Krakowa – coraz mocniejsza

Kwantowa dystrybucja klucza to technologia zabezpieczeń, która znacząco wyprzedza obecne standardy. Jest to ważny krok w kierunku przeciwdziałania potencjalnym zagrożeniom związanym z wykorzystaniem przyszłych komputerów kwantowych do łamania obecnie używanych szyfrów. Tym samym technologie QKD przyczyniają się do zabezpieczania krytycznej infrastruktury Krakowa. Wdrożenie technologii kwantowej dystrybucji kluczy szyfrujących jest efektem współpracy pomiędzy Akademią Górniczo-Hutniczą a Urzędem Miasta Krakowa, rozszerzając jedno z głównych założeń Cyfrowej Tarczy Krakowa tj.: zapobiegać zagrożeniom w cyberprzestrzeni, zanim te nastąpią.

– To nie jest projekt na dziś, ale inwestycja w bezpieczeństwo Krakowa na dekady. Po podpisaniu listu intencyjnego z AGH mówiliśmy, że chcemy wyprzedzać zagrożenia w cyberprzestrzeni – dziś pokazujemy, że potrafimy przejść od deklaracji do konkretnych, przełomowych wdrożeń. Kwantowa dystrybucja kluczy to najwyższy możliwy standard ochrony danych, oparty na prawach fizyki, a nie na kompromisach. Dzięki współpracy z AGH i Cyfronetem Kraków buduje swoje cyfrowe bezpieczeństwo w oparciu o naukę, innowacje i odpowiedzialność za dane mieszkańców, stając się jednocześnie aktywnym uczestnikiem europejskich działań na rzecz bezpiecznej komunikacji przyszłości – podkreśla Aleksander Miszalski, prezydent Krakowa.

Jak to działa?

– Technologia kwantowej dystrybucji kluczy szyfrujących bazuje na zabezpieczonej kwantowo komunikacji pary urządzeń. Po stronie Cyfronetu jedno urządzenie generuje klucze za pomocą kwantowego generatora liczb losowych. Klucze są następnie przekazywane do szyfratora, który szyfruje połączenie pomiędzy Urzędem Miasta a Cyfronetem. Po stronie Urzędu Miasta Krakowa znajduje się drugie urządzenie, odbierające klucze i przekazujące je do lokalnego szyfratora, który odpowiada za szyfrowanie i rozkodowanie danych po stronie Urzędu – wyjaśnia Marek Chorąży, specjalista w zakresie technologii kwantowych w Cyfronecie, główny inżynier wdrożenia systemu QKD.

Technologia kwantowej dystrybucji kluczy szyfrujących jest uznawana za niemożliwą do złamania. Bazuje na prawach fizyki, a nie na matematycznych zabezpieczeniach. Oznacza to, że próba podsłuchu lub kopiowania klucza natychmiast go niszczy lub zniekształca, tym samym wykrywana jest obecność kogoś, kto chce przejąć przesyłaną wiadomość czy dane. W odróżnieniu od klasycznego szyfrowania, klucz nie istnieje jako obiekt, który można skopiować, ale jest generowany i przesyłany w sposób zależny od zasad mechaniki kwantowej, eliminując w ten sposób możliwość jego przechwycenia bez wykrycia.

Element większego ekosystemu

Stworzona przez specjalistów z Cyfronetu infrastruktura ochrony przesyłanych danych dodatkowo poszerza usługi oferowane przez tę jednostkę dla środowiska akademickiego i przedsiębiorców. – Dbając o bezpieczeństwo przetwarzanych danych, połączenie QKD utworzono również pomiędzy głównym i zapasowym centrum danych Cyfronetu. Mając na uwadze współdzielenie zasobów obliczeniowych naszych superkomputerów Ares, Athena i Helios, a także systemów pamięci masowych, bardzo ważne jest, aby dane przesyłane między dwiema lokalizacjami posiadały najwyższy możliwy poziom zabezpieczeń – podkreśla K. Krawentek, zastępca dyrektora ACK Cyfronet AGH.

Europejska infrastruktura

Wdrożenie technologii kwantowej dystrybucji kluczy szyfrujących w Krakowie pomiędzy Cyfronetem i Urzędem Miasta Krakowa jest elementem znacznie większej inicjatywy w Europie. Jej celem nie jest budowa pojedynczych bezpiecznych połączeń, lecz rozległej sieci obejmującej obszar Unii Europejskiej. W Polsce połączenia takie budowane są w ramach projektu PIONIER-Q i obejmują połączenia pomiędzy centrami komputerów dużej mocy oraz wybranymi ośrodkami miejskich sieci komputerowych. W latach 2026–2028 w ramach części europejskiej inicjatywy *European Quantum Communication Infrastructure* (EuroQCI), Cyfronet wraz z partnerami będzie budował połączenia do krajów położonych blisko Polski. Tworzona sieć ma chronić wrażliwe dane i infrastrukturę krytyczną poprzez integrację systemów bazujących na zasadach mechaniki kwantowej z istniejącą infrastrukturą komunikacyjną, zapewniając dodatkową warstwę bezpieczeństwa.

Twórcą kwantowej dystrybucji kluczy szyfrujących jest prof. Artur Ekert, pionier kryptografii

kwantowej, na co dzień związany z Uniwersytetem Oksfordzkim i Narodowym Uniwersytetem w Singapurze. Był jednym z pierwszych naukowców, który zaproponował wykorzystanie praw mechaniki kwantowej do zapewnienia bezpieczeństwa przesyłania informacji. Inżynierowie z AGH bazują zatem na metodzie odkrytej w 1991 roku. Technologia kwantowej dystrybucji kluczy szyfrujących nie jest jednak szeroko wykorzystywana, ale rozwija się i ma strategiczne znaczenie dla bezpieczeństwa infrastruktury krytycznej, komunikacji satelitarnej czy ochrony danych.