

# POLSKI RZĄD POZNA KODY ŹRÓDŁOWE HUAWEI?

---

Huawei zaoferował polskiemu rządowi dostęp do kodów źródłowych w celu sprawdzenia ich pod kątem bezpieczeństwa. Argumentem jest chęć wzmocnienia zaufania do rozwiązań chińskiej firmy. Te słowa padły podczas konferencji prasowej Huawei w Warszawie, której gościem był Jaap Meijer, Cyber Security Officer w Huawei Netherlands.

## Cyberbezpieczeństwo okiem Huawei

Holenderski przedstawiciel Huawei zarysował podejście przedsiębiorstwa do cyberbezpieczeństwa. Na wstępie podkreślił, że chińska firma znajduje się obecnie w orbicie zainteresowań mediów na całym świecie. Jego zdaniem jest to nieuzasadnione, a cyberbezpieczeństwo stanowi bardzo ważny element strategii Huawei. Firma jest zawsze chętna do współpracy z rządami, klientami oraz partnerami w celu wspólnej walki z zagrożeniami z cyberprzestrzeni. Nigdy też komercyjne interesy nie będą miały pierwszeństwa nad cyberbezpieczeństwem – zapewnił. Przytoczył tym samym słowa założyciela firmy Huawei Rena Zhengfeia.

Jaap Meijer przedstawił wizję Huawei, który zamierza dostarczyć bezpieczne usługi cyfrowe do każdej organizacji, domu i jednostki w połączonym świecie. Cyberbezpieczeństwo jest wbudowane w usługi firmy oraz narzędzia chińskiej firmy.

Jej strategia oparta jest na 5 filarach. Pierwszym z nich są badania i rozwój. Tutaj chińska firma bierze aktywny udział w pracach światowych organizacji zajmujących się standaryzacją i certyfikacją oraz korzysta również z najlepszych praktyk bezpieczeństwa przemysłu. Drugim filarem jest bezpieczeństwo łańcucha dostaw opierające się na odpowiednim zarządzaniu zasobami, sprawdzaniu jakości materiałów i światowej logistyce. Trzeci element to usługi cyberbezpieczeństwa, czyli dbanie o bezpieczeństwo infrastruktury, aplikacji, danych, przeprowadzenie audytów oraz kodeks postępowania w obszarze bezpieczeństwa i ochrony danych. Czwarty filar skupia się na zasobach ludzkich odpowiedzialnych za cyberbezpieczeństwo. Celem jest tutaj zatrudnianie osób, które nie prowadzą żadnej nielegalnej działalności. Ostatni element to zarządzanie podatnościami, które znajdują się w sprzęcie i oprogramowaniu Huawei.

Według Jaap Meijera esencją cyberbezpieczeństwa, nie tylko w obszarze 5G, powinno być minimalizowanie ryzyka dostarczenia sprzętu z podatnościami, które mogą negatywnie wpłynąć na dostępność, integrację oraz poufność usług. Cyberbezpieczeństwo nie powinno być ani się rozpoczynać ani kończyć na granicach państwowych. Mówimy przecież o usługach globalnych i światowym łańcuchu dostaw.

## Huawei a „tylne furtki”

Jaap Meijer mówił również, że Huawei stworzył i ciągle doskonali system zapewnienia bezpieczeństwa końcowemu użytkownikom. Podkreślił, że chińska firma nigdy nie tworzyła i nie będzie tworzyć „tylnych furtek”, nawet jeżeli zostanie poproszona przez chiński rząd. Zaznaczył też, że jego zdaniem

takie furtki bardzo łatwo może wykryć operator telekomunikacyjny korzystający ze sprzętu 5G. Omawiając tę problematykę wspomniał również o chińskim prawie, które rzekomo miałyby zobowiązywać krajowe firmy do współpracy z wywiadem i kontrwywiadem Państwa Środka. Meijer podkreślił, że to nieprawda, a chińskie prawo nie obowiązuje poza terytorium Chin. Co więcej to właśnie firmy z tego kraju muszą dostosować się do regulacji europejskich w postaci RODO. Podkreślił też, że bezpieczeństwo jest zapewniane przez standaryzację w obszarze 5G oraz zarządzanie operacyjne siecią 5G.

W jego opinii cyberbezpieczeństwo nie jest zmartwieniem jednego państwa czy firmy, ale problemem ponadnarodowym. Wszyscy uczestnicy, począwszy od rządów po przemysł muszą zrozumieć, że cyberbezpieczeństwo jest światowym problemem, który wymaga przeprowadzenia analizy ryzyka, wdrożenia najlepszych praktyk i międzynarodowej współpracy. W opinii Holendra usunięcia Huawei z 5G nie rozwiąże problemu bezpieczeństwa w Polsce, z którymi należy się zmierzyć wprowadzając tę technologię.

Holenderski przedstawiciel Huawei poinformował również, że planowane jest otwarcie dedykowanego European Cyber Security Center w Brukseli 5 marca. Zadaniem będzie komunikacja z rządami państw UE, innymi firmami, indywidualnymi użytkownikami w celu wypracowania i usprawnienia już obowiązujących regulacji w zakresie bezpieczeństwa oraz ochrony prywatności. Nacisk ma zostać położony na transparentność. Placówka ma się składać z:

- Experience Center, w którym będą przedstawiane rozwiązania Huawei w obszarze cyberbezpieczeństwa,
- Knowledge Hub, którego zadaniem będzie komunikacja i współpraca w obszarze dzielenia się najlepszymi praktykami.
- Evaluation Center, gdzie będą prowadzone testy bezpieczeństwa produktów chińskiej firmy.

## **Huawei niezależny od rządu**

Huawei jest spółką prywatną, która w całości stanowi własność pracowników i nie ma żadnych związków z chińskim rządem – poinformowano podczas konferencji. Z informacji udostępnionych przez firmę wynika, że urządzenia Huawei używane są od 30 lat przez ponad 3 miliardów klientów z ponad 170 krajów na całym świecie. Przedsiębiorstwo przez ten czas miało nie odnotować żadnych incydentów bezpieczeństwa.

Podczas spotkania zaprezentowano również dane dotyczące polskiego rynku. Huawei do tej pory zainwestował w Polsce ponad 5 miliardów. W ciągu trzech lat zapłacił 630 milionów złotych podatków, w tym 250 milionów złotych w samym 2018 roku. Ponadto chińska firma dokonała zakupów na kwotę 800 milionów złotych w przeciągu ostatnich 3 lata. W samym 2018 roku na ten cel przeznaczono 360 milionów. W ciągu następnych trzech lat Huawei ma zamiar zainwestować dodatkowe 2 mld złotych. Chińczycy przedstawili również informacje o wielkości zatrudnienia. Obecnie pracuje u nich prawie 1000 osób w Polsce, a pośrednie firma przyczynia się do tworzenia łączenia ponad 3000 miejsc pracy.

W 2008 roku Huawei przeniósł z Rumunii do Polski regionalne centrum na Europę Środkowo-Wschodnią i kraje nordyckie, zarządzające operacjami w 28 europejskich krajach.

Zdaniem przedstawicieli chińskiej firmy, Huawei w technologii 5G wyprzedza konkurencję o około 12-18 miesięcy. Firma podpisała kontrakty na rozwój sieci 5G z ponad 30 państwami, w tym 18 europejskimi takimi jak Wielka Brytania, Niemcy, Włochy, Portugalia czy Finlandia. Firma miała wystąpić do klientów ponad 25 tys. stacji bazowych.

Huawei przeprowadził również badania na temat skutków wykluczenia firmy Huawei z Polski. Czas

wdrożenia tej infrastruktury wydłużyłyby się w Polsce o co najmniej 12 do 18 miesięcy w stosunku do innych państw. Koszt jej realizacji wdrożenia wzrósłby o 8,5 miliarda euro, a rachunki osób korzystających z tej infrastruktury wzrosłyby o minimum 100 proc.