Dziennik Gazeta Prawna
11.03.19 nr: 49 str. 8 nakład: 47000 egz.

PREZENTACJA: FORUM GOSPODARCZE TIME

NIE UNIKNIEMY CYBERATAKÓW

prof. Jacek Leśkow, dyrektor NASK – Państwowego Instytutu Badawczego

Jacek Leśkow: Rozwój nowych technologii sprzyja wzrostowi przestępczości w sieci. Rolą NASK jest nie tylko minimalizowanie jej skutków, ale zapobieganie. Dlatego stawiamy na innowacje i edukację

W rezultacie cyberataków światowa gospodarka traci ponad 600 mld dol. rocznie. Prognozuje się, że do 2030 r. kwota ta ulegnie podwojeniu. Czy Polska ma coraz większy w tym udział?

Zadałbym raczej pytanie, czy Polska ma już istotny udział w ochronie przed cyberatakami. I tu odpowiedziałbym, że tak. Mamy już własne algorytmy i prototypy urządzeń, które dbają o bezpieczeństwo w różnych sferach. Przykładem może być niedawne udaremnienie kilku poważnych cyberataków w instytucjach publicznych. Przygotowaliśmy i wdrożyliśmy także otoczenie legislacyjne – od sierpnia 2018 roku działa przygotowana przez Ministerstwo Cyfryzacji ustawa o krajowym systemie cyberbezpieczeństwa, która wprowadziła ważne mechanizmy budowy cyberochrony Rzeczpospolitej.

Czy rozwój gospodarki 4.0 zwiększa prawdopodobieństwo cyberataków?

Zdecydowanie tak. Weźmy rynek pojazdów autonomicznych, który przeżywa rozwój. Wystarczy przeprowadzić atak na system w tych pojazdach, który rozpoznaje znaki drogowe, by doprowadzić do dramatycznych skutków. Podobne niebezpieczeństwo rodzi rozwój internetu rzeczy. Im więcej komunikowania się urządzeń, tym więcej możliwości złośliwych ataków. Nie można jednak zapominać o benefitach wynikających z rozwoju gospodarki 4.0. Dlatego zagrożenia nie powinny przesłaniać korzyści. Podobnie jest w przypadku sieci 5G. Wciąż jest do rozwiązania dużo dylematów związanych z bezpieczeństwem, ale sieć 5G zdecydowanie podniesie jakość życia. Stworzy możliwość porozumiewania się różnych urządzeń, co ułatwi funkcjonowanie człowiekowi.

Mówi pan o dylematach. Jaka jest w tej kwestii rola NASK w obszarze cyfryzacyjnym?

Głównym wyzwaniem, ale i misją naszej instytucji jest budowanie świadomości nie tylko zwykłych obywateli, ale i urzędników, właścicieli firm na temat cyberbezpieczeństwa, internetu rzeczy czy rewolucji przemysłowej 4.0. Drogą do tego są prace badawczo-rozwojowe, którym musi towarzyszyć edukacja.

Podam przykład. Przygotowujemy platformę cyfrową, która stanowić będzie jednolity system obiegu dokumentów dla wszystkich podmiotów polskiej administracji publicznej. Ma zacząć działać od 2021 r. Zanim to jednak nastąpi, trzeba przygotować pracowników do nowych rozwiązań. Oznacza to zmianę ich sposobu myślenia i podejścia do pracy. Przestają być ważne kompetencje ściśle techniczne, a znaczenia nabierają różnego rodzaju umiejętności miękkie.

Nad czym jeszcze pracujecie?

Jednym z kluczowych projektów jest budowa Ogólnopolskiej Sieci Edukacyjnej – programu Ministerstwa Cyfryzacji, realizowanego przez NASK. To odpowiedź na potrzebę zintegrowanego działania na rzecz cyfryzacji polskich jednostek oświatowych. OSE połączy ze sobą w jeden organizm ponad 26 tys. szkół. Dzięki temu za 2-3 lata uczeń będzie mógł uczestniczyć w zajęciach z dowolnego miejsca w kraju i korzystać z nowoczesnych narzędzi edukacyjnych. Warunkiem do tego jest zapewnienie powszechnego i równego dostępu do bardzo szybkiego, bezpiecznego i bezpłatnego internetu dla szkół. Trzeba też przygotować kadrę nauczycielską na szykujące się zmiany. W opinii niektórych pedagogów postępująca rewolucja oznaczać będzie mniejsze zapotrzebowanie na ich usługi. Tymczasem trzeba im uświadomić, że dzięki OSE będą mogli skoncentrować się na przygotowaniu się do zajęć, na zwiększeniu kontaktów z młodzieżą, otrzymają nowe możliwości kształcenia uczniów.

Kolejnym wyzwaniem dla Polski, ale i Europy Środkowo-Wschodniej jest uświadamianie opinii publicznej i decydentom, iż cyberprzestrzeń może być wykorzystana do agresji. Nie trzeba już rakiet. Wystarczy atak powodujący odcięcie dostępu do gazu, energii czy wody, by sparaliżować cały kraj czy nawet region. Dlatego tak ważna staje się wymiana doświadczeń. To ważny element przeciwdziałania ewentualnym cyberatakom. W Polsce dużą rolę w tym zakresie ma do spełnienia Ministerstwo Cyfryzacji, w którym funkcjonuje pełnomocnik rządu ds. cyberbezpieczeństwa minister Karol Okoński.

Jakie plany w związku z tym ma NASK?

Stawiamy na współpracę z zagranicznymi partnerami dotyczącą usług cyfrowych, cyberbezpieczeństwa oraz badań i rozwoju. Za trzy tygodnie udaję się do Stanów Zjednoczonych, gdzie odwiedzę cztery ośrodki akademickie i spotkam się z naukowcami. Chcę nawiązać współpracę z polonijnymi naukowcami. Myślę, że możemy skorzystać z ich wiedzy z zakresu sztucznej inteligencji i jej zastosowań w cyberbezpieczeństwie.

Widzę NASK jako instytucję, która może absorbować wiedzę z instytucji światowych. Dlatego będziemy rozwijać współpracę z ośrodkami badawczymi, uczelniami, a także przedsiębiorstwami z wielu miejsc na świecie. Obecnie realizujemy również wiele projektów naukowych z partnerami zagranicznymi.

Jak widzi pan miejsce swojej instytucji w walce z cyberzagrożeniami?

Obok ustawowych zadań, związanych ze współtworzeniem przez nas krajowego systemu cyberbezpieczeństwa, myślę, że NASK mógłby stać się też brokerem dla polskiego przemysłu i firm w naszej części świata. Jako instytut badawczy, mający wsparcie Ministerstwa Cyfryzacji, może zostać integratorem rozwiązań, z których będą korzystać inni. Szczególnie że w Polsce mamy trzy resorty i mnóstwo ośrodków, których działalność koncentruje się wokół sztucznej inteligencji, która powinna odgrywać coraz większą rolę w obszarze cyber. Tym bardziej, że w Unii Europejskiej, wzorem Stanów Zjednoczonych, powinniśmy dążyć do stworzenia otwartej przestrzeni dostępu do danych tam gdzie jest to tylko możliwe. Wszystko w celu poprawy jakości życia obywateli. Oczywiście wiążą się z tym cyberzagrożenia. Trzeba jednak szukać rozwiązań, które pozwolą poradzić sobie z przeciwnościami. My chcemy mieć w tym udział. Zmiany cywilizacyjne w związku z postępem technologicznym są nieuniknione. Trzeba o tym mówić i pokazywać nowe rozwiązania. PAO

Materiał powstał przy współpracy z NASK