

<https://www.bbn.gov.pl/pl/wydarzenia/7958,Policyjna-uczelnia-w-Szczytnie-zorganizowala-warsztaty-z-cyberbezpieczenstwa.html>

06.07.2025, 10:46

10.07.2017

Policyjna uczelnia w Szczytnie zorganizowała warsztaty z cyberbezpieczeństwa

W Wyższej Szkole Policji w Szczytnie ruszyła w poniedziałek Letnia Szkoła Cyberbezpieczeństwa. Uczestnikami pierwszej edycji warsztatów są głównie osoby odpowiedzialne za teleinformatyczną ochronę infrastruktury krytycznej. W wydarzeniu uczestniczył zastępca szefa BBN minister Dariusz Gwizdała.

Według organizatorów, szkolenia mają pogłębić wiedzę przedstawicieli operatorów infrastruktury krytycznej, odpowiedzialnych za teleinformatyczne bezpieczeństwo obiektów i instalacji, które pełnią kluczową rolę dla państwa. Mają również pomóc im wypracować praktyczne modele ochrony takich systemów i rozwiązania w zakresie współdziałania z administracją państwową, policją i innymi służbami zwalczającymi cyberprzestępczość i cyberterroryzm.

Jak powiedział w wystąpieniu zastępca szefa BBN, ataki do jakich doszło w ostatnim czasie na Ukrainie pokazały, że zagrożenia, które jeszcze niedawno uważano za teoretycznie możliwe, dziś stały się naszą codziennością. Rodzi to pytania, jak Polska by sobie poradziła w sytuacji ataku np. na system energetyczny czy finansowy?

Minister D. Gwizdała, odnosząc się do wyników prac działającego w ubiegłym roku przy BBN zespołu ds. bezpieczeństwa cyberprzestrzeni RP, powiedział, że w celu zapewnienia bezpieczeństwa systemów komputerowych stanowiących tzw. układ nerwowy państwa, stosowanie dobrych praktyk najlepiej uzupełnić o rozwiązania obligatoryjne - wraz z zestawem minimalnych wymagań i procedur dostosowanych do specyfiki poszczególnych sektorów infrastruktury krytycznej. Ponadto opracowanie minimalnych standardów i egzekwowanie ich przestrzegania powinno być zadaniem dla regulatorów branżowych nadzorujących poszczególne sektory.

Zastępca szefa BBN przypomniał, że bezpieczeństwo cyberprzestrzeni nie jest wyłącznym zadaniem państwa. Odpowiedzialność spoczywa także na indywidualnych użytkownikach i sektorze prywatnym, szczególnie operatorach infrastruktury krytycznej. Dlatego kształtując system cyberbezpieczeństwa RP należy stworzyć warunki, w których firmy będą widziały korzyści ze współpracy z państwem, a wydatki na cyberbezpieczeństwo będą traktowały jako inwestycję, a nie zbędny koszt.

Uczestniczący w inauguracji I Letniej Szkoły Cyberbezpieczeństwa podsekretarz stanu w MSWiA Tomasz Zdzikot mówił, że to przedsięwzięcie wpisuje się w przyjętą przez rząd strategię cyberbezpieczeństwa. Jak podkreślał, szczególną rolę w budowaniu kadr i kompetencji ma odgrywać Wyższa Szkoła Policji w Szczytnie, która od 20 lat specjalizuje się w tej dziedzinie.



fot. wspol.edu.pl



fot. wspol.edu.pl

Według Zdzikota, ze względu na to, że znaczna część infrastruktury krytycznej znajduje się w rękach prywatnych, ogromne znaczenie ma współpraca administracji państwowej ze wszystkimi podmiotami i instytucjami, które odpowiadają za jej utrzymanie i zabezpieczenia.

"Dlatego też zaprosiliśmy państwa właśnie tu i właśnie ten temat podejmujemy jako pierwszy, bo uważamy, że jest to po prostu konieczne, a z punktu widzenia bezpieczeństwa państwa - najbardziej istotne" - mówił do uczestników warsztatów.

Jak zapowiedział, Letnia Szkoła Cyberbezpieczeństwa będzie miała kolejne edycje. Policyjna uczelnia ze Szczytna ma również uruchomić od października studia z informatyki na kierunku bezpieczeństwo. Planowane są też podyplomowe studia z zakresu zwalczania cyberzagrożeń w sektorze bankowym, a także związane z bezpieczeństwem dokumentów publicznych.

Minister cyfryzacji Anna Streżyńska powiedziała natomiast, że cieszy ją tak duże zróżnicowanie uczestników Letniej Szkoły Cyberbezpieczeństwa. Jak mówiła, wierzy, że to początek współpracy, która obejmie osoby z bardzo różnych organizacji, jednostek administracji państwowej, przedsiębiorstw, samorządów terytorialnych czy organizacji pozarządowych.

Zdaniem minister to niezbędne, żeby zachować zasady cyberbezpieczeństwa i skutecznie bronić się przed przestępcami, którzy - jak zauważyła - współdziałają ze sobą, by być jak najlepiej poinformowanymi co do możliwych sposobów prowadzenia swojej działalności.

"Po naszej stronie też musi być stworzony mur współpracy, który łączy kompetencje i swoiste spojrzenia na cyberbezpieczeństwo, jakimi dysponuje każda z naszych organizacji" - podkreśliła.

W pierwszej edycji Letniej Szkoły Cyberbezpieczeństwa uczestniczy ok. 40 osób, głównie pracowników pionów bezpieczeństwa spółek Skarbu Państwa działających w obszarach zaopatrzenia w energię, surowce energetyczne i paliwa, łączności oraz sieci teleinformatycznych.

Zaplanowane na pięć dni zajęcia - pod hasłem "Cyber Odyseja - wyzwania XXI wieku" - mają formę wykładów i warsztatów. Prowadzą je polscy i zagraniczni eksperci rekrutujący się m.in. z organów ścigania, środowiska nauki i biznesu. Podczas warsztatów omówione zostaną przypadki zdiagnozowanych cyberataków i wypracowane rekomendacje służące zwiększeniu bezpieczeństwa teleinformatycznego.

Letnia Szkoła Cyberbezpieczeństwa została zorganizowana przez WSPol w Szczytnie i MSWiA we współpracy z Rządowym Centrum Bezpieczeństwa, Polską Wytwórnią Papierów Wartościowych S.A. i Polskimi Sieciami Elektroenergetycznymi S.A. Patronat nad tym przedsięwzięciem objęli: Minister Spraw Wewnętrznych i Administracji, Szef Biura Bezpieczeństwa Narodowego, Minister Cyfryzacji, Minister Obrony Narodowej i Prokurator Krajowy.

Infrastruktura krytyczna (IK) to rzeczywiste i cybernetyczne systemy (obiekty, urządzenia bądź instalacje) niezbędne do minimalnego funkcjonowania gospodarki i państwa. Obejmuje systemy zaopatrzenia w energię, surowce energetyczne i paliwa, zaopatrzenia w żywność, w wodę, a także systemy: łączności, sieci teleinformatycznych, finansowe, ochrony zdrowia, transportowe, ratownicze oraz produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych.

[Tweetnij](#)