**Lidia Maria Jedlińska**
Wojewódzka Biblioteka Publiczna w Krakowie

Artykuł zamieszczony na platformie edukacji dorosłych EPALE (6.12.2017) **TUTAJ>>>**

# CYBERSEC 2017 – wyzwania, rekomendacje

W październiku 2017 roku Kraków ponownie stał się centrum międzynarodowej dyskusji o bezpieczeństwie w cyberprzestrzeni. CYBERSEC (link is external), bo o nim mowa, to tworzenie platformy współpracy pomiędzy rządami, organizacjami międzynarodowymi oraz kluczowymi podmiotami sektora prywatnego w celu wzmocnienia cyberbezpieczeństwa Europy.

Podczas dwudniowych spotkań kilkuset uczestników i ponad 100 panelistów występujących w czterech ścieżkach tematycznych wypracowuje praktyczne rekomendacje.

Na szczególną uwagę zasługuje organizacja dodatkowej sesji CYBERSEC for SENIORS, której tematyka dotyczy bezpieczeństwa w sieci osób starszych.

1) Ścieżka Państwo: „*budowanie wielopodmiotowej współpracy oraz wspieranie procesu tworzenia strategii publicznych związanych z cyfryzacją i cyberbezpieczeństwem*".

Trudno aktualnie znaleźć państwo, które nie opierałoby swojego funkcjonowania o cyberprzestrzeń. Wymaga to dostosowania polityk publicznych do nowych realiów, budowania współpracy angażującej wszystkich interesariuszy, dostosowania prawa, tworzenia efektywnych strategii publicznych, tworzenia mechanizmów ochrony infrastruktury krytycznej i zarządzania kryzysowego. Kluczowym elementem procesu budowania zaufania w ceberprzestrzeni jest jego świadomość wśród decydentów wysokiego szczebla.

Tematami omawianymi tym panelu były takie, jak ochrona infrastruktury krytycznej, strategie cyberbezpieczeństwa państw, współpraca międzynarodowa na rzecz cyberbezpieczeństwa, walka z terrorystami wykorzystującymi cyberprzestrzeń.

2) Ścieżka Obrona: „*zwiększanie zdolności do cyberobrony w obliczu narastających zagrożeń wynikających z funkcjonowania współczesnych* w *państw w cyberprzestrzeni*".

Efektywny system cyberbezpieczeństwa jest podstawą skutecznej obrony współczesnych państw. Operatorzy powinny rozpowszechniać dobre praktyki oraz oferować narzędzia i rozwiązania ramowe, umożliwiające demaskowanie przypadków manipulacji danymi.

Tematyka spotkania w tym panelu oscylowała głównie wokół funkcjonowanie NATO w cyberprzestrzeni, współpracy NATO i UE w zakresie cyberbezpieczeństwa, ochrony przed cyberatakami jako elementami walki hybrydowej czy walki informacyjnej prowadzonej w wirtualu.

3) Ścieżka Przyszłość: „*definiowanie trendów, szans i wyzwań, a także tworzenie cyberinnowacji i rozwój społeczeństwa informacyjnego*”.

Cyberprzestrzeń wywiera wpływ na wszystkie aspekty życia społeczno-gospodarczego. Dlatego, aby skutecznie przeciwdziałać zagrożeniom nie wystarczą umiejętności z zakresu ICT, ale należy stworzyć dyscyplinę naukową zajmującą się obserwacją aktualnych trendów i prognozowaniem kierunków rozwoju w przyszłości.

Rekomendacje dotyczyły innowacyjnych, bezpiecznych rozwiązań służących społeczeństwom informacyjnym i były tworzone na bazie dyskusji o m.in. sztucznej inteligencji, zmianach w potrzebach i zachowaniach użytkowników sieci, cyfrowych zasobach kadrowych. Wskazywano na konieczność szukania i kreowania talentów, wywodzących się z różnych grup społecznych oraz opracowania potrzebnych umiejętności interdyscyplinarnych, uczenia się od siebie nawzajem. To właśnie poprzez odpowiednie wykorzystanie wiedzy możemy dziś przewidywać, a co za tym idzie – unikać zagrożeń. Ważną rolę odgrywa również innowacyjność rozumiana jako promowanie rozwoju i współpracy.

4) Ścieżka Biznes: „*określenie roli sektora prywatnego w zapewnianiu cyberbezpieczeństwa oraz analiza kluczowych trendów związanych z rynkiem cyberproduktów i usług”.*

Celem tej ścieżki było wypracowanie rekomendacji obejmujących zaangażowanie biznesu w proces umacniania bezpieczeństwa cyberprzestrzeni. Dyskusja toczyła się wokół takich tematów jak: bezpieczny Internet Rzeczy (ang. Internet of Things), przyszłe potrzeby rynku produktów i usług dla cyberbezpieczeństwa, budowanie jednolitego rynku cyfrowego UE, walka przedsiębiorstw z cyberzagrożeniami.

Równolegle z panelami odbyły się warsztaty edukacyjne CYBERSEC for SENIORS (link is external) skierowane do osób powyżej 55. roku życia. Wzięło w nich udział ok. 100 seniorów posiadających podstawowe umiejętności korzystania z komputera i Internetu. W programie znalazły się wykłady przedstawicieli nauki, biznesu, rządu. Ich celem było zwrócenie uwagi osób starszych na ceberzagrożenia, poszerzanie ich kompetencji cyfrowych oraz informacje o jakości i dostępności do e-usług publicznych. Spotkanie było także okazją do zadawania pytań oraz dyskusji.

Szczególne zainteresowanie wzbudził temat „*Fake news. Dlaczego nabieramy się na nieprawdziwe treści w sieci, czym to może grozić oraz jak się przed tym ustrzec*?” (dr Dominik Batorski; Centrum Modelowania Matematycznego i Komputerowego na Uniwersytecie Warszawskim) oraz „*Jak używać Profilu Zaufanego – o korzyściach dla obywatela”* (Urszula Świetlińska, Centralny Ośrodek Informatyki).

Warsztaty są odpowiedzią na rosnące zainteresowanie seniorów i potrzeby debaty o ich bezpieczeństwie w sieci.

Oby więcej było organizowanych tego typu przedsięwzięć!

Organizator Konferencji:

Instytut Kościuszki - niezależny, pozarządowy instytut naukowo-badawczy, think tank o charakterze non profit, założony w 2000 r. W prace Instytutu zaangażowani są naukowcy, pracownicy polskiej i europejskiej administracji oraz praktycy działalności publicznej i społeczno-gospodarczej. Instytut tworzy ekspertyzy i rekomendacje programowe dla europejskich i polskich instytucji publicznych.

**dr Lidia Maria Jedlińska** - główny specjalista ds. integracji społecznej w Dziale Edukacji, Nauki i Badań Wojewódzkiej Biblioteki Publicznej w Krakowie, koordynator projektów krajowych i międzynarodowych koncentrujących się na problematyce przeciwdziałania wykluczeniu społecznemu i cyfrowemu (pomysłodawca Programu „Szkoła @ktywnego Seniora-S@S"); organizator warsztatów, seminariów, konferencji z zakresu edukacji obywatelskiej; promotor współpracy międzypokoleniowej, ambasador EPALE i LABIB