

3. Czy mówiąc o wdrożeniach UKSC mówimy wszyscy o tym samym? Czym jest KSC i jak jest rozumiane przez różne podmioty?

Moderator: Jakub Dysarz, naczelnik Wydziału Certyfikacji i Szkoleń, Departament Cyberbezpieczeństwa, Ministerstwo Cyfryzacji

Ustawa o krajowym systemie cyberbezpieczeństwa weszła w życie w 2018 r., przyćmiona nieco przez RODO. Miała o wiele węższy zakres stosowania i objęła o wiele mniej podmiotów. Mimo pierwotnych przewidywań, okazała się wyzwaniem nawet dla dużych podmiotów. Mimo wąskiego zakresu, odnoszącego się tylko do usług kluczowych, zrozumiałe było, że konieczne jest zabezpieczenie całej organizacji. Jednym z głównych wyzwań jest brak odpowiednich, przeszkolonych kadr, zwłaszcza z zakresu bezpieczeństwa automatyki przemysłowej. Problem jest też podejście ustawy nastawione na usługi, a nie produkcję, co wymagało też zmian organizacyjnych w niektórych firmach. Dla firm, które nie posiadały zdolności do samodzielnego wdrożenia ustawy, dotkliwy był koszt wyniesienia kosztów wdrożenia na zewnątrz. Jako pomocne wskazano zastosowanie preaudytu celem rozeznania się, czego tak naprawdę brakuje w organizacji do osiągnięcia pożądanego poziomu cyberbezpieczeństwa. W wielu podmiotach wdrożenie ciągle trwa – zwłaszcza tych, które mają rozległe obszarowo i skomplikowane systemy automatyki przemysłowej. Ciekawym zjawiskiem jest fakt, że niektóre firmy zaczęły stosować wzór szablonu audytu, przygotowany przez ISSA Polska Stowarzyszenie ds. Bezpieczeństwa Systemów Informacyjnych oraz Instytutem Audytorów Wewnętrznych IIA Polska we współpracy z Ministerstwem Cyfryzacji. Szablon, mimo iż niewiążący, okazał się być obowiązującym standardem dla organizacji.