Europejski system certyfikacji produktów sektora teleinformatycznego

Krzysztof POLITOWSKI

Departament Cyberbezpieczeństwa Ministerstwa Cyfryzacji

Ministerstwo Cyfryzacji

Podstawowe definicje

Certyfikacja

- formalny proces realizowany przez stronę trzecią, mający na celu potwierdzenie zgodności wyrobu z wymaganiami

Akredytacja

- formalny proces realizowany przez podmiot upoważniony przez organ władzy państwowej, mający na celu potwierdzenie zdolności jednostki oceniającej do realizacji swoich zadań

Jednostka oceniająca

- Akredytowany podmiot, który wykonuje czynności z zakresu oceny zgodności, w tym wzorcowanie, **badanie**, **certyfikację** i inspekcję

Podstawy prawne

- **Ustawa z dnia 30 sierpnia 2002 r. o systemie oceny zgodności (Dz. U. 2016 poz. 665 z późn. zm.);**
- **Rozporządzenie Parlamentu Europejskiego i Rady (WE) NR 765/2008 z dnia 9 lipca 2008 r. ustanawiające wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylające rozporządzenie (EWG) nr 339/93;**

Kalendarium wybranych inicjatyw UE w zakresie cyberbezpieczeństwa

- 2006 – Strategia Bezpieczeństwa Społeczeństwa Informacyjnego
- 2009 – Komunikat KE ws. Ochrony Krytycznej Infrastruktury Informatycznej (CIIP)
- 2011 – Kolejny Komunikat KE ws. Ochrony Krytycznej Infrastruktury Informatycznej (CIIP)
- 2013 – Europejska Strategia Cyberbezpieczeństwa
- 2014 – Rozporządzenie 910/2014 (eIDAS)
- 2016 – Dyrektywa 1148/2016 (NIS)
- 2016 – Opracowanie planu działań mających na celu opracowanie europejskich ram certyfikacji i ich przedstawienie z końcem roku 2017

Polskie stanowisko ws. europejskich ramy certyfikacji bezpieczeństwa wyrobów sektora TI

- **Wprowadzenie europejskiej klasyfikacji wyrobów sektora TI pod względem poziomu zaufania (assurance level), co pozwoli na wprowadzenie różnych modeli certyfikacji:**
  - **Deklaracji zgodności na poziomie niskim i średnim,**
  - **Certyfikacji na zgodność z profilami ochrony (Protections Profiles - PP) na poziomie wysokim.**
- **Stosowanie wspólnych profili ochrony (PP) ustanawianych na podstawie powszechnego konsensusu i dostępnych na zasadzie free-of-charge.**
- **Wzajemnego uznawania certyfikatów na europejskim wspólnym rynku cyfrowym z wyłączeniem wyrobów mających zastosowanie w obszarze bezpieczeństwa narodowego.**
- **Oznaczanie certyfikowanych wyrobów znakiem rozpoznawalnym również na rynkach poza obszarem UE.**

Polskie kalendarium systemu certyfikacji

2004, po rozpatrzeniu wszystkich za i przeciw Polska postanowiła nie przystępować do CCRA;

Czerwiec 2016, Minister Cyfryzacji aprobowała rozpoczęcie projektu mającego ustanowić i wdrożyć krajowy system oceny i certyfikacji bezpieczeństwa wyrobów sektora TI bazującego na Polskiej Normie PN-ISO/IEC 15408 (Common Criteria);

Celem projektu jest stworzenie w pełni operacyjnego krajowego system oceny i certyfikacji bezpieczeństwa wyrobów sektora TI, który spełni wymagania umożliwiające przystąpienie do SOGIS-MRA jako pełnoprawnego członka (Certificate Authorized Member);

Czas trwania projektu obliczony jest na 36 miesięcy.

System certyfikacji wyrobów ICT w Polsce

PCA

jako podmiot akredytujący

Minister Cyfryzacji jako organizator systemu

NASK

jako podmiot certyfikujący

IŁ PIB

jako laboratorium badawcze

ITI EMAG

jako laboratorium badawcze

inne laboratoria badawcze

Dziękuję za uwagę

krzysztof.politowski@mc.gov.pl