

Andrzej Kupiec
CTO
Xsecures

„Edukacja jako fundament budowy Cyberbezpiecznego Państwa”

1. Edukacja jako strategiczna inwestycja: W obliczu zagrożeń cyfrowych i dążenia do suwerenności technologicznej, edukacja jest kluczowym fundamentem budowy Cyberbezpiecznego Państwa, zapewniającym zarówno odporność, jak i niezależność w cyfrowej sferze. Bez wykwalifikowanych kadr nie istnieje skuteczne cyberbezpieczeństwo ani pełna suwerenność.
2. Fundament Techniczny - Podstawa Operacyjna:
 - Kształcenie specjalistów od szerokopojętej infrastruktury IT, bezpiecznego kodowania (SDLC), reagowania na incydenty i technik ofensywno-defensywnych jest niezbędne do budowy i ochrony podstawowych usług cyfrowych państwa.
 - Rozwój kompetencji w obszarze DevSecOps – integrowania bezpieczeństwa na każdym etapie cyklu życia oprogramowania – stanowi o bezpieczeństwie tworzonych przez państwo rozwiązań.
3. Eksperckie Kompetencje - Zarządzanie, Audyt i Zgodność:
 - Edukacja musi skupiać się na kształceniu kadr zdolnych do zarządzania ryzykiem, audytowania systemów i procesów (z uwzględnieniem bezpieczeństwa oprogramowania), oraz wdrażania polityk bezpieczeństwa zgodnie z najlepszymi praktykami.
 - Kluczowe jest zrozumienie i stosowanie wymogów prawnych (RODO, prawo dot. infrastruktury krytycznej) oraz standardów, co gwarantuje zgodność działania państwa z prawem (compliance).
4. Strategiczna Architektura - Projektowanie Bezpieczeństwa i Suwerenności:
 - Niezbędne jest kształcenie wizjonerów i strategów tworzących bezpieczne architektury IT i oprogramowania, które wspierają cele państwa, zapewniając jego suwerenność technologiczną i prawną.
 - Edukacja w zakresie tworzenia kompleksowych architektur pozwala na integrację bezpieczeństwa, prawa i procesów rozwojowych, budując spójny i odporny system cyfrowy.
5. Edukacja jako narzędzie budowania świadomości i suwerenności:
 - Kompleksowa edukacja buduje świadomość sytuacyjną (zagrożeń, zależności, konsekwencji) i prawną u wszystkich odbiorców – od obywateli po kadrę zarządzającą.
 - Inwestycja w krajową kadrę specjalistyczną zorientowaną na bezpieczeństwo i zgodność prawną jest kluczem do suwerenności technologicznej i prawnej państwa.

Podsumowanie:

Cyberbezpieczne Państwo opiera się na edukacji, która kształtuje kompetentnych specjalistów, skutecznych menedżerów, świadomych prawnie architektów i wizjonerów. Tylko takie holistyczne podejście zapewnia narodową odporność, zgodność z prawem i prawdziwą suwerenność w cyfrowym świecie.