CYBERODPORNOŚĆ

Normatywny kontekst cyberodporności w rozwiązaniach e-Zdrowia

Bartłomiej Michalak, Krzysztof Świtała (Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie)

XVI Konferencja Bezpieczeństwo w Internecie - Cyberodporność

Warszawa 5 grudnia 2024 r.

Organizatorzy: UKSW, Ministerstwo Cyfryzacji

Partner wspierający: NASK

Partner merytoryczny: SAMSUNG

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2024/2847 z dnia 23 października 2024 r. w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi oraz w sprawie zmiany rozporządzeń (UE) nr 168/2013 i (UE) 2019/1020 i dyrektywy (UE) 2020/1828

Akt o cyberodporności (ang. Cyber Resilience Act)

E-Zdrowie

- WHO definiuje e-zdrowie jako efektywne kosztowo i bezpieczne wykorzystanie technologii informacyjnych i komunikacyjnych (ICT) we wspieraniu zdrowia i dziedzin związanych ze zdrowiem, w tym usług opieki zdrowotnej, nadzoru zdrowotnego, literatury na temat zdrowia oraz edukacji zdrowotnej, wiedzy i badań.
- Istnieją wyraźne dowody na rosnący wpływ e-zdrowia na świadczenie opieki zdrowotnej na całym świecie oraz na to, w jaki sposób sprawia ono, że systemy opieki zdrowotnej są bardziej wydajne i lepiej reagują na potrzeby i oczekiwania ludzi.

WHO eHealth definition (https://www.emro.who.int/health-topics/ehealth/).

CRA a NIS2 i ochrona zdrowia

- Chociaż proponowany akt dotyczący cyberodporności obejmuje produkty z elementami cyfrowymi wprowadzane do obrotu, celem dyrektywy NIS2 2022/2555 jest zapewnienie wysokiego poziomu cyberbezpieczeństwa usług świadczonych przez podmioty niezbędne i istotne.
- W dyrektywie NIS2 zobowiązano państwa członkowskie do zapewnienia, aby podmioty niezbędne i istotne objęte zakresem jej stosowania, takie jak **świadczeniodawcy opieki zdrowotnej lub dostawcy usług w chmurze oraz podmioty administracji publicznej**, wprowadzały odpowiednie i proporcjonalne środki techniczne, operacyjne i organizacyjne w zakresie cyberbezpieczeństwa.

Usługi w chmurze obliczeniowej a cyberbezpieczeństwo (COM(2022) 454)

- W dyrektywie NIS 2 zobowiązano Komisję do przyjęcia aktów wykonawczych określających wymogi techniczne i metodyczne dotyczące tych środków w terminie 21 miesięcy od daty wejścia w życie tej dyrektywy w odniesieniu do niektórych rodzajów podmiotów, takich jak dostawcy usług w chmurze.
- W odniesieniu do wszystkich innych podmiotów Komisja może przyjąć akt wykonawczy określający wymogi techniczne i metodyczne, jak również wymogi sektorowe. Ramy te zapewnią wdrożenie specyfikacji technicznych i środków podobnych do zasadniczych wymogów cyberbezpieczeństwa określonych w akcie dotyczącym cyberodporności również w odniesieniu do projektowania, opracowywania i postępowania w przypadku wykrycia podatności **oprogramowania dostarczanego jako usługa (oprogramowanie jako usługa)**.
- Może to być na przykład środek zapewniający wysoki poziom cyberbezpieczeństwa w takich przypadkach jak systemy **elektronicznej dokumentacji medycznej (EHR)**, w tym gdy są dostarczane w postaci oprogramowania jako usługa (SaaS) lub opracowywane w ramach instytucji zdrowia publicznego (wewnętrznie), zgodnie z proponowanym **rozporządzeniem w sprawie europejskiej przestrzeni danych dotyczących zdrowia** (COM (2022) 197) *(motyw 31 i art. 24 ust. 4 CRA).*

CRA a wyroby medyczne

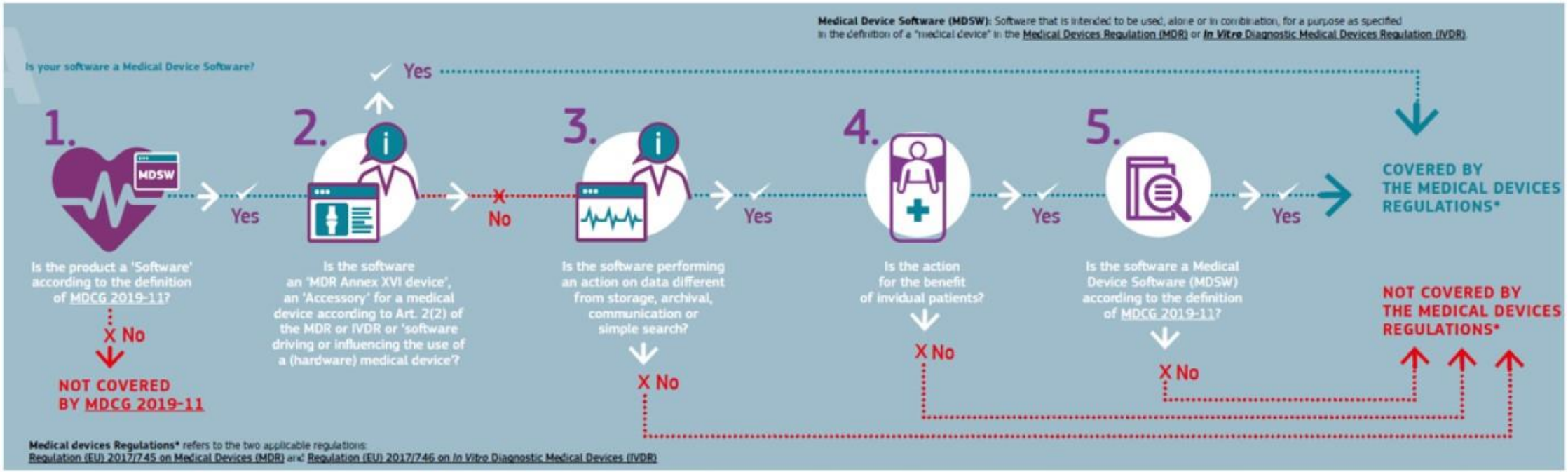
- Motyw 12 CRA - proponowane rozporządzenie nie będzie miało zastosowania do produktów z elementami cyfrowymi objętych zakresem **rozporządzenia (UE) 2017/745 dotyczącego wyrobów medycznych stosowanych u ludzi oraz wyposażenia takich wyrobów** oraz rozporządzenia (UE) 2017/746 dotyczącego wyrobów medycznych do diagnostyki in vitro stosowanych u ludzi oraz wyposażenia takich wyrobów, ponieważ oba te rozporządzenia zawierają wymogi dotyczące wyrobów, w tym dotyczące oprogramowania i ogólnych obowiązków producentów, obejmujące cały cykl życia produktów, a także procedury oceny zgodności.

Definicja art. 2 ust. 1 MDR (UE) 2017/745

„wyrób medyczny” oznacza narzędzie, aparat, urządzenie, oprogramowanie, implant, odczynnik, materiał lub inny artykuł przewidziany przez producenta do stosowania – pojedynczo lub łącznie – u ludzi do co najmniej jednego z następujących szczególnych zastosowań medycznych: — diagnozowanie, profilaktyka, monitorowanie, przewidywanie, prognozowanie, leczenie lub łagodzenie choroby, — diagnozowanie, monitorowanie, leczenie, łagodzenie lub kompensowanie urazu lub niepełnosprawności, — badanie, zastępowanie lub modyfikowanie budowy anatomicznej lub procesu lub stanu fizjologicznego lub chorobowego, — dostarczanie informacji poprzez badanie *in vitro* próbek pobranych z organizmu ludzkiego, w tym pobranych od dawców narządów, krwi i tkanek, i który nie osiąga swojego zasadniczego przewidzianego działania środkami farmakologicznymi, immunologicznymi lub metabolicznymi w ludzkim ciele lub na nim, ale którego działanie może być wspomagane takimi środkami. Następujące produkty są również uznawane za wyroby medyczne: — wyroby do celów kontroli poczęć lub wspomagania poczęcia, — produkty specjalnie przeznaczone do czyszczenia, dezynfekcji lub sterylizacji wyrobów, o których mowa w art. 1 ust. 4, oraz wyrobów, o których mowa w akapicie pierwszym niniejszego punktu.

Oprogramowanie jako wyrób medyczny

Decision steps to assist qualification of Medical Device Software (MDSW)



CYBERODPORNOŚĆ

Dziękujemy za uwagę.

UKSW

Ministerstwo Cyfryzacji

Naukowe Centrum Prawno-Informatyczne

SAMSUNG

NASK