Cyber Resilience Act – kolejna cegła w unijnym murze cyberbezpieczeństwa

Jakub Kukulski
Młodszy Analityk The Opportunity

16.02.2024

30 listopada 2023 roku Rada, Komisja i Parlament Europejski osiągnęły porozumienie w sprawie tekstu ustawy Cyber Resilience Act (CRA). Legislacja ma wejść w życie na wiosnę 2024 roku, a jej przepisy mają zacząć obowiązywać stopniowo, aż do pełnej implementacji w 2027 roku.

Zapisy ustawy obejmują producentów sprzętów elektronicznych (urządzenia smart, zegarki, zabawki, itd.) i twórców oprogramowań. Celem CRA jest podniesienie poziomu bezpieczeństwa cybernetycznego produktów poprzez wymuszenie na producentach uwzględnienia odpowiednich zasad już na etapie projektowania towarów i usług oraz w całym cyklu życia produktu. Legislacja zobowiązuje producentów do dostarczania ocen ryzyka cyberbezpieczeństwa ich produktów odpowiednim organom (państwowym lub unijnej agencji ENISA [The European Union Agency for Cybersecurity]) i zapewnienia wsparcia produktom, u których zostałyby znalezione podatności mogące być wykorzystane przez cyberprzestępców.

W wypadku niestosowania się do przepisów, CRA nakłada na producentów grzywny w wysokości do 15 milionów euro lub 2,5% ich globalnego rocznego obrotu za poprzedni rok podatkowy, w zależności od tego, która z tych kwot jest wyższa.

Według ENISA koszty cyberprzestępstw na świecie osiągną wysokość 10,5 bilionów dolarów rocznie w 2025 roku. Jednym z głównych zagrożeń, którym CRA ma przeciwdziałać są ataki typu ransomware. ENISA zanotowała wzrost ilości tego typu ataków na terenie UE o 21% między 2022 a 2023 rokiem. Najbardziej podatnymi na ataki są małe i mikroprzedsiębiorstwa (do 50 osób zatrudnionych), które według European Digital SME Alliance najczęściej padają ofiarą ataków typu ransomware (86% wszystkich dotkniętych firm w Europie).

Pomimo obaw części sektora OSS dotyczących odpowiedzialności prawnej za wolno dystrybuowane oprogramowania, raportowanie podatności produktu jak i zapewnienie im wsparcia to praktyki wdrożone na szeroką skalę chociażby przez firmy z Singapuru.

CRA jest bardzo istotny dla cyberbezpieczeństwa w Europie Środkowo-Wschodniej. Region posiada prężnie rozwijający się sektor IT, zaś Polska, według zestawienia firmy GBS World, była w 2022 roku drugą (po Indiach) najbardziej atrakcyjną lokalizacją dla outsourcingu usług IT. Polski sektor IT może skorzystać na CRA, pod warunkiem, że uda się ujednolicić krajowy system cyberbezpieczeństwa i utworzyć na poziomie krajowym ciało, do którego mogłyby spływać raporty poszczególnych firm.