Wkład ZPP w konsultacje Komisji Europejskiej w sprawie aktu dotyczącego cyberodporności - nowe przepisy cyberbezpieczeństwa produktów cyfrowych i usług pomocniczych

Komisja Europejska rozpoczęła 16 marca 2022 roku konsultacje społeczne w sprawie aktu dotyczącego cyberodporności - nowych przepisów cyberbezpieczeństwa produktów cyfrowych i usług pomocniczych.[1] Akt ten został zapowiedziany przez przewodniczącą KE Ursulę von der Leyen we wrześniu 2021 roku w jej przemówieniu o stanie Unii.[2] Wraz z rozpoczęciem konsultacji Komisja wydała również wezwanie do przedstawienia dowodów na potrzebę oceny skutków regulacji. Akt dotyczący cyberodporności ma uzupełnić rozporządzenie delegowane z dnia 29 października 2021 r. wydane na podstawie dyrektywy w sprawie urządzeń radiowych poprzez ustanowienie zoptymalizowanych wymogów dotyczących cyberbezpieczeństwa obejmujących szeroki wachlarz produktów cyfrowych oraz ich usług pomocniczych.[3] Ponadto, regulacja uzupełni istniejące ramy prawne, które obejmują Dyrektywę NIS[4], Unijny Akt o Cyberbezpieczeństwie[5] oraz wpiszę się w przyszłą Dyrektywę NIS 2.[6]

Uzasadnieniem dla konsultowanego projektu jest zapobieżenie cyberatakom. Jako przyczynę takiego stanu rzeczy zostały wskazane brak odpowiednich zabezpieczeń oraz niedostateczna reakcja na luki w zabezpieczeniach przez cały cykl życia produktu. Ponadto, Komisja Europejska wskazuje na brak wystarczającej informacji w zakresie bezpieczeństwa produktu. Czynnikami wpływającymi na obniżenie poziomu zabezpieczeń jest brak zachęt ekonomicznych oraz wykwalifikowanych specjalistów ds. bezpieczeństwa.

Regulacja ma na celu ustanowienie uproszczonych wymagań dotyczących bezpieczeństwa obejmujących szeroki zakres produktów cyfrowych oraz usług pomocniczych. Nowe akt ma regulować namacalne produkty cyfrowego (zarówno przewodowe jak i bezprzewodowe) oraz oprogramowanie niewbudowane, które zostanie objęte postanowieniami aktu w całym cyklu życia produktu.

Według Komisji Europejskiej obecne ramy regulacyjne są niedostateczne, ponieważ nie pokrywają zakresem wszystkich produktów cyfrowych (np. oprogramowania niewbudowanego) a także nie określają szczegółowych wymogów bezpieczeństwa obejmujących cały cykl życia produktów. Biorąc pod uwagę powyższe Komisja rozważa różne kierunki polityk mających na celu zapobieganie cyberzagrożeniom, takie jak: doraźne rozwiązania regulacyjne w istniejącym prawodawstwie, horyzontalna interwencja regulacyjna, wprowadzenie dobrowolnych środków (w tym rozwój systemów certyfikacji), mieszane podejście regulacyjne lub utrzymanie statusu quo.

Związek Przedsiębiorców i Pracodawców z zadowoleniem przyjmuje propozycję Komisji mającą na wzrost cyberbezpieczeństwa Europejskich użytkowników. Wyróżniliśmy dwa zasadnicze aspekty, do

[1]https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services_pl

[2] https://ec.europa.eu/info/strategy/strategic-planning/state-union-addresses/state-union-2021_pl

[3] https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32022R0030&from=PL

[4] https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32016L1148&from=BG

[5] https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32019R0881&from=EN

[6]https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union

których uregulowania dąży propozycja aktu. Po pierwsze, jest to badanie poziomu bezpieczeństwa z perspektywy usług świadczonych użytkownikom końcowym. Jest to rozumiane jako bezpieczeństwo danych użytkowników oraz dostępu (także niezawodność dostępu) do oferowanych usług, szczególnie poprzez sieci publiczne. Po drugie, bezpieczeństwo sieci publicznych przez zagrożeniami związanymi z cyberatakami. Należy tutaj uwzględnić ataki od wewnątrz sieci, do których mogą doprowadzić luki bezpieczeństwa w oprogramowaniu. Ważny jest tutaj także kontekst polskiej Ustawy o Krajowym Systemie Cyberbezpieczeństwa i stworzonych przez nią ram regulacyjnych.[7]

W ocenie ZPP szczególnie istotne jest rozwijanie sprzętu i oprogramownaia do sieci radiodostępowych. Należy zaznaczyć, że dostęp do urządzeń radiodostępowych (RAN) operatora jest ograniczony. Urządzenia te znajdują się fizycznie w siedzibie operatora gdzie są chronione przed ingerencją osób trzecich. Ponadto, urządzenia te pracują w wydzielonej sieci operatora, która zapewnia bezpieczeństwo dostępu zdalnego. Chroni on dostępu do tej wydzielonej sieci przed nieuprawnionym dostępem. W związku z powyższym operator posiada pełną kontrolę nad dostępem do urządzeń RAN.

Bezpieczeństwo danych użytkownika jest opisane w odpowiedniej dla wybranej techniki radiodostępu specyfikacji technicznej i ustawień operatora (2G/3G/4G/5G). Za sprawą specyfikacji technicznej określane są algorytmy szyfrujące i zabezpieczające oraz długości kluczy. Dzięki temu nie ma różnic pomiędzy dostawcami sprzętu w zakresie zapewnienia bezpieczeństwa zarówno użytkownikom końcowym jak i samej sieci.

Biorąc pod uwagę powyższe uważamy, że kwestie zapewnienia odpowiedniego poziomu bezpieczeństwa powinny znajdować się w gestii operatorów, albowiem posiadają oni najlepiej dopasowane narzędzia, aby móc dynamicznie reagować na powstałe zagrożenia. Podobnie, z uwagi na istniejące obecnie mechanizmy ochrony bezpieczeństwa stosowane w poszczególnych podmiotach opowiadamy się za pozostawieniem uprawnienia do przeprowadzania audytów tym jednostkom.

W naszej opinii operatorzy mają najlepszą wiedzę w zakresie technik ochrony bezpieczeństwa własnych sieci oraz mają w tym najlepszy interes, aby utrzymać bezpieczeństwo własnych środowisk, co potwierdza dotychczasowa praktyka. Rekomendujemy dokonanie weryfikacji na okoliczność czy proponowane w specyfikacji technicznej rozwiązania i algorytmy dotyczące bezpieczeństwa są wystarczające dla zapewnienia cyberbezpieczeństwa produktów cyfrowych i usług pomocniczych.

[7] https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/T/D20181560L.pdf