Warszawa, dnia 28 stycznia 2021 r.

Departament Cyberbezpieczeństwa
Kancelaria Prezesa Rady Ministrów

STANOWISKO

ZWIĄZKU PRACODAWCÓW BRANŻY INTERNETOWEJ INTERACTIVE ADVERTISING BUREAU (IAB POLSKA) W/S PROJEKTU ZASTĄPIENIA DYREKTYWY NIS NOWĄ REGULACJĄ – TJ. PRZYJĘCIA DYREKTYWY PARLAMENTU EUROPEJSKIEGO I RADY W SPRAWIE ŚRODKÓW NA RZECZ WYSOKIEGO WSPÓLNEGO POZIOMU CYBERBEZPIECZEŃSTWA NA TERYTORIUM UNII - W WERSJI Z DNIA 16 GRUDNIA 2021 R.

Szanowni Państwo,

W odpowiedzi na zaproszenie do składania stanowisk i opinii odnoszących się do projektu zastąpienia dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dalej: „**dyrektywa NIS”**) nową dyrektywą - dyrektywą Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (dalej: „**dyrektywa NIS2”**), Związek Pracodawców Branży Internetowej IAB Polska (dalej: „**IAB Polska**”) pragnie przedstawić swoje stanowisko.

IAB Polska, jako zrzeszenie ponad 200 członków, wśród których znajdują się m.in. największe portale internetowe, sieci reklamowe, domy mediowe i agencje interaktywne, z dużym zadowoleniem przyjmuje możliwość wyrażenia opinii na temat przedmiotowego dokumentu. Naszym celem jest zaakcentowanie potrzeby zapewnienia wyważonych przepisów, które będą sprzyjały rozwojowi innowacyjnej gospodarki. Liczymy na dalszą współpracę z Państwem w tej ważnej kwestii.

1. Wstęp

Dyrektywa NIS to pierwszy kompleksowy unijny akt w obszarze cyberbezpieczeństwa, którego celem było stworzenie jednolitych ram regulacji tego zagadnienia, a tym samym zbliżenie przepisów państw członkowskich w zakresie odporności sieci i systemów informatycznych. W praktyce, dyrektywa stała się impulsem do przyjęcia krajowych przepisów, szczególnie potrzebnym z uwagi na fakt, że cyberbezpieczeństwo nie było dotąd przedmiotem szerokiego zainteresowania ustawodawców.

Niemniej 4 lata obowiązywania dyrektywy NIS pokazały, że przyjęte w niej podejście okazało się niewystarczające. Zarzuty dotyczyły m.in.:

- znaczących rozbieżności pomiędzy podejściem poszczególnych krajów do sposobu wyznaczania operatorów usług kluczowych, co miało w praktyce wpływ na podmioty

świadczące usługi na ich rzecz (w przypadku polskiej regulacji, nie mogły zidentyfikować czy mają do czynienia z takim operatorem, o ile sam operator nie przekazał im tej informacji),
- konieczności tworzenia odrębnych ścieżek postępowania na wypadek incydentów klasyfikowanych na podstawie odrębnych regulacji (w przypadku polskiej implementacji przepisów dyrektywy, w skrajnych przypadkach, konieczne jest utrzymywanie odrębnych procedur dla zgłoszeń na podstawie RODO, prawa telekomunikacyjnego oraz ustawy o krajowym systemie cyberbezpieczeństwa),
- braku wystarczających ram dla współpracy między podmiotami objętymi regulacją, dotyczącej wymiany wiedzy i doświadczeń w obszarze cyberbezpieczeństwa.

W świetle powyższego, przegląd dyrektywy NIS oraz propozycję nowej regulacji dyrektywy NIS2 należy co do zasady ocenić pozytywnie, gdyż w dużej mierze odpowiada na zgłoszone postulaty. Biorąc jednak pod uwagę fakt, że regulacja ta ma charakter dyrektywy, a nie rozporządzenia, kluczowa okaże się jej implementacja w polskim porządku prawnym.

2. Uwagi

W kontekście powyższego, należy zwrócić uwagę, że dyrektywa NIS2 może objąć szerszy krąg podmiotów – rozszerza bowiem sektory i rodzaje działalności na takie, które nie podlegały dotychczas przepisom w zakresie cyberbezpieczeństwa. Z perspektywy członków IAB Polska, istotne jest rozszerzenie regulacji w obszarze cyberbezpieczeństwa na serwisy społecznościowe, a także dostawców publicznych sieci łączności elektronicznej i dostawców usług łączności elektronicznej, jeśli są one powszechnie dostępne, a także – analogicznie jak w dyrektywie NIS – objęcie regulacją wyszukiwarek internetowych, dostawców usług cloud computing oraz internetowych platform handlowych.

W tym kontekście, kluczowe jest określenie podejścia w przypadku podmiotów oferujących różnego rodzaju usługi, potencjalnie kwalifikujące te podmioty zarówno jako *essential entities* jak i *important entities*. Dotyczy to zwłaszcza podmiotów w sektorze infrastruktury cyfrowej, które mogą oferować np. zarówno usługi chmury obliczeniowej, jak i usługi w zakresie internetowych platform handlowych. Dyrektywa NIS2 powinna przesądzać, czy w takim przypadku należy zastosować podwyższone wymogi, czy też badać, który przedmiot działalności ma charakter dominujący, lub też w inny sposób odpowiedzieć na powyższe wątpliwości.

W odniesieniu do zakresu podmiotowego dyrektywy NIS istotny jest także fakt, że zmianie ulega sposób kwalifikacji podmiotu jako podlegającego regulacji dyrektywy – na gruncie dyrektywy NIS2 brana jest pod uwagę tylko ogólna skala działalności (średnie i duże przedsiębiorstwo), nie jest badany natomiast próg istotności skutku zakłócającego incydentu dla świadczenia usługi kluczowej, a w jego ramach różne aspekty ilościowe (np. ilość obsługiwanych domen w przypadku usług DNS). Rodzi to obawę, że identyczne wymogi zostaną postawione podmiotom oferującym swoje usługi kilku klientom, jak i podmiotom oferującym te usługi kilku tysiącom klientów. Podobnie, wymogi mogą być identyczne dla tych podmiotów, które oferują swoje usługi podmiotom z kategorii *essetial entities*, jak i podmiotom z grupy *important entities*, a także odbiorcom niepodlegającym dyrektywie NIS2.

Mając powyższe na uwadze, o ile IAB Polska ma świadomość istotnej roli tych podmiotów i potrzeby zapewnienia cyberbezpieczeństwa systemom wykorzystywanym do świadczenia przez nich usług i prowadzenia działalności, o tyle zwraca uwagę na potrzebę wyważenia nałożonych na te podmioty obowiązków i poddaje pod uwagę zróżnicowanie ich pod kątem odbiorców usług (zarówno w zakresie kryteria ilościowego, jak i rodzaju odbiorcy). Zgodnie z projektem dyrektywy NIS2, kraje członkowskie powinny zapewnić, że podmioty objęte regulacją podejmą odpowiednie i proporcjonalne środki techniczne i organizacyjne w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych, które podmioty te wykorzystują przy świadczeniu swoich usług. W tym zakresie, IAB Polska postuluje także brak wprowadzania sztywnych wymogów w tym zakresie, lecz podejście w całości oparte na ryzyku. Byłoby to również spójne z uwagami zgłaszanymi dotychczas do aktów wykonawczych do ustawy o krajowym systemie cyberbezpieczeństwa, które doprowadziły do zmiany rozporządzeń w tym zakresie.

Podobne uwagi należy odnieść do obowiązku stworzenia krajowych mechanizmów dotyczących współpracy i wymiany informacji. O ile ramy regulacji w tym zakresie mogą okazać się potrzebne, aby zmotywować podmioty objęte regulacją do współpracy, o tyle wszystkie szczegółowe kwestie dotyczące funkcjonowania takich struktur powinny pozostać w gestii ich członków. Takie podejście może dać impuls do tworzenia organizacji na wzór ISAC, które w Polsce nie były dotąd popularne. Jako jedną z obaw, uczestnicy krajowego systemu cyberbezpieczeństwa wskazywali właśnie brak określenia struktur działania takich inicjatyw.

Współpraca i wymiana informacji powinna być również zapewniona w relacji między właściwymi organami, również w kontekście zgłaszania incydentów oraz naruszeń na gruncie poszczególnych regulacji. Biorąc pod uwagę, że incydenty mają często złożony charakter oraz w znacznej części dotyczą również danych osobowych, pod rozwagę poddajemy możliwość stworzenia jednej ścieżki ich obsługi z perspektywy relacji podmiotu zobowiązanego – właściwego organu. W naszej ocenie mogłoby to ułatwić obsługę incydentów, nie nakładając jednocześnie nadmiernych obciążeń na podmioty zobowiązane. Byłoby to również wyrazem kompleksowego podejścia do tej kwestii, w przeciwieństwie do podejścia opartego na rozproszonych regulacjach i odrębnych ścieżkach informowania, tym samym przyczyniając się do sprawniejszej wymiany informacji i doświadczeń w obszarze cyberbezpieczeństwa.

Z poważaniem,

Włodzimierz Schmidt

Prezes Zarządu

Związek Pracodawców Branży Internetowej IAB Polska
ul. Puławska 39 lok. 77 02-508 Warszawa tel. +48 22 415 54 44 fax +48 22 212 87 74
www.iab.org.pl