aut. Andrzej Kozłowski 26.01.2021

BIUROKRATYCZNA KŁODA CZY SZANSA NA WZMOCNIENIE CYBERBEZPIECZEŃSTWA UE? EKSPERCI SPIERAJĄ SIĘ O PROJEKT DYREKTYWY NIS2

Czy projekt opinii dyrektywy NIS2 spełnia wymania rynku? O jakie aspekty powinien zostać poszerzony? O ocenę dokumentu poprosiliśmy ekspertów.

16 grudnia 2020 r. Komisja Europejska ogłosiła tzw. Pakiet cyberbezpieczeństwa. W jego skład, oprócz nowej Strategii Cyberbezpieczeństwa UE, wchodzi także projekt zmiany dyrektywy NIS, czyli podstawowego unijnego dokumentu regulującego cyberbezpieczeństwo na poziomie europejskim. O ocenę proponowanych zmian oraz wskazanie brakujących elementów poprosiliśmy ekspertów. Komentarza do sprawy zdecydowali się udzielić:

- Mariusz Busiło; kancelaria Bącal, Busiło.
- Katarzyna Chałubińska-Jentkiewicz, dyrektorka Centrum Polityki Cyberbezpieczeństwa (ACPC) Akademii Sztuki Wojennej;
- Eksperci Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni;
- Michał Kanownik, Prezes Zarządu ZIPSEE – Cyfrowa Polska;
- Ireneusz Piecuch, Senior Partner i współzałożyciel kancelarii DGTL
- Krzysztof Silicki; Zastępca Dyrektora NASK, Dyrektor ds. Cyberbezpieczeństwa i Innowacji.

Czy w Pani/Pana opinii projekt dyrektywy NIS2 spełnia wymagania rynku? Jakie problematyczne aspekty dostrzega Pani/Pan w nowych przepisach?

"Zmiany zaproponowane przez KE są bardzo ambitne" **- o**cenia Krzysztof Silicki, Zastępca Dyrektora NASK**.** "Przede wszystkim wyraźnie wydać zbliżenie kwestii bezpieczeństwa fizycznego i teleinformatycznego. NIS 2 rozszerza zakres podmiotowy dotychczasowej dyrektywy m.in. o administrację publiczną, sektor żywności, ścieki, produkcja wyrobów medycznych, komputerowych, elektronicznych i optycznych;, zarządzanie odpadami oraz przestrzeń kosmiczną a także szerzej traktuje niektóre sektory (m.in. rozszerzenie zakresu infrastruktury cyfrowej)" - dodaje.

Z Krzysztofem Silickim zgadza się Michał Kanownik, który szczególnie chwali Dyrektywę za objęcie jej zakresem sektora telekomunikacyjnego i publicznego. W opinii Kanownika "postulat pozwoli na stworzenie spójnych europejskich ram prawnych cyberbezpieczeństwa obejmujących zarówno sektor ICT, jak i telekomunikacyjny. Dziś przecież poziom bezpieczeństwa systemów informatycznych jest ściśle powiązany z bezpieczeństwem telekomunikacyjnym – np. w sytuacji, gdy operatorzy telekomunikacyjni pełnią jednocześnie funkcje operatorów usług kluczowych czy dostawców usług cyfrowych" - przypomina Prezes Zarządu ZIPSEE - Cyfrowa Polska. Mniej optymistyczna co do wprowadzenia sektora telekomunikacyjnego w obszar dyrektywy NIS2 jest profesor Chałubińska-

Jentkiewicz. W jej opinii "nowelizacja Dyrektywy może stwarzać pole do kolizji z przepisami wynikającymi z innych przepisów m.in. Dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej, gdzie zagadnienia bezpieczeństwa sieci oraz usług telekomunikacyjnych zostały także ustalone, a w praktyce wymogi są realizowane od wielu lat".

Sceptycznie o zakładanych w projekcie karach wypowiada się Mariusz Busiło. Jak stwierdził, "dyrektywa NIS2 podąża tropem RODO, a receptą na przestrzeganie nowych przepisów mają być drakońsko wysokie kary. Czy poprawi to rzeczywiste cyberbezpieczeństwo, czy będzie kolejną biurokratyczną kłodą w rozwoju europejskich innowacji zobaczymy w najbliższych pięciu latach. Patrząc na dotychczasowy wpływ RODO na ochronę naszych danych osobowych, jestem raczej sceptyczny" - podkreśla Busiło.

Potencjalne skutki wprowadzenia dyrektywy NIS w Polsce przedstawia Ireneusz Piecuch. Jego zdaniem "oprócz obowiązków przeprowadzania standardowych audytów pojawią się audyty celowe związane z oceną ryzyka. Konieczność dostarczania określonej dokumentacji na życzenie uprawnionych organów. Krajowe organy nadzoru mają zostać wyposażone w uprawnienia, które wskazują na to, że w Polsce pojawi się kolejny obok UOKiK, UKE oraz UODO organ posiadający bardzo daleko idące uprawnienia" - przewiduje Piecuch.

Pomimo kilku wątpliwości, optymistycznie do dyrektywy podchodzi prof. Chałubińska-Jentkiewicz, która wskazała, że "nowa regulacja może służyć zwiększeniu odporności na cyberataki, jeżeli zostanie skutecznie implementowana przez państwa członkowskie".

O jakie aspekty powinna zostać poszerzona dyrektywa NIS2?

Eksperci Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni zwracają uwagę, że "przedmiotowa dyrektywa powinna być adaptatywna w zakresie sojuszów i koalicji, które nie będą pozostawały bez znaczenia dla wielopoziomowego i wielopodmiotowego cyberbezpieczeństwa, a podmioty pozostające w ścisłej kooperacji i interoperacyjności nie będą podmiotami wyłącznie europejskimi (np. partnerzy z NATO)."

Profesor Chałubińska-Jentkiewicz zwraca uwagę z kolei na kwestie poziomu kar. Podkreśla ona, że "dyrektywa przewiduje także wysokie kary finansowe dla podmiotów nie realizujących obowiązków we właściwy sposób. Kary te mają wynosić maksymalnie co najmniej 10000000 EUR lub do 2% całkowitego rocznego światowego obrotu przedsiębiorstwa, w zależności od tego która kwota jest wyższa. Poziom tych kar może być szczególnie dotkliwy dla mniejszych przedsiębiorców, którzy dopiero wchodzą do systemu cyberbezpieczeństwa. Być może potrzebna byłaby tu odpowiednia gradacja kar" - rekomenduje dyrektorka Centrum Polityki Cyberbezpieczeństwa Akademii Sztuki Wojennej. W opinii Michała Kanownika projekt Dyrektywy powinien zostać rozszerzony o regulacje dotyczące mechanizmów przeciwdziałania kradzieży tożsamości.

Innego zdania jest Mariusz Busiło, który zwraca uwagę na zły kierunek całej dyrektywy. W jego opinii "regulacja powinna być nastawiona na szeroką edukację społeczną (słynne zdanie Kevina Mitnicka:“łamałem ludzi nie hasła”), promowanie postaw bezpiecznych oraz udzielania wsparcia, a zamienia się w mechanizm represjonowania ofiar".

Eksperci różnie oceniają nowy projekt dyrektywy NIS2. Wskazują na objęcie sektora telekomunikacyjnego jako pozytywną zmianę, podkreślając, że bez objęcia operatorów telekomunikacyjnych tymi regulacjami nie da się potem stworzyć pełnego i kompatybilnego krajowego systemu cyberbezpieczeństwa. Jednocześnie jednak zauważają, że może to doprowadzić do kolizji z innymi przepisami unijnymi ustanawiającej Europejski kodeks łączności elektronicznej,

gdzie zagadnienia bezpieczeństwa sieci oraz usług telekomunikacyjnych zostały także ustalone. Obawę ekspertów wzbudzają również wysokie kary. Zdaniem Mariusza Busiło jest to w ogóle błędne założenie samej dyrektywy, która nie powinna bazować tylko na strachu. Profesor Chałubińska-Jentkiewicz widzi zagrożenie, że taką sama wysokość kar zostanie nałożona na duże i małe przedsiębiorstwa, co może doprowadzić do bankructwa tych ostatnich.

NIS 2 to istotna legislacyjna odpowiedź na wzrost liczby incydentów w sieci, która zostanie wdrożona do krajowego porządku prawnego dopiero za dwa lata. Czy w takim razie będzie ona w dalszym ciągu adekwatna do poziomu ówczesnego poziomu rozwoju cyfrowej gospodarki?

Pełne odpowiedzi udzielone przez ekspertów znajdują się poniżej:

- Mariusz Busiło; kancelaria Bącal, Busiło.
- Katarzyna Chałubińska-Jentkiewicz, dyrektorka Centrum Polityki Cyberbezpieczeństwa (ACPC) Akademii Sztuki Wojennej;
- Eksperci Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni;
- Michał Kanownik, Prezes Zarządu ZIPSEE – Cyfrowa Polska;
- Ireneusz Piecuch, Senior Partner i współzałożyciel kancelarii DGTL;
- Krzysztof Silicki; Zastępca Dyrektora NASK, Dyrektor ds. Cyberbezpieczeństwa i Innowacji.