INFORMACJA PRAWNA

DOTYCZĄCA DYREKTYWY PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/1148 Z DNIA 6 LIPCA 2016 ROKU W SPRAWIE ŚRODKÓW NA RZECZ WYSOKIEGO WSPÓLNEGO POZIOMU BEZPIECZEŃSTWA SIECI I SYSTEMÓW INFORMATYCZYCH NA TERYTORIUM UE DALEJ: „DYREKTYWA NIS".

Dyrektywa NIS weszła w życie w sierpniu 2016 roku. Od tego czasu Państwa Członkowskie UE mają 21 miesięcy na jej implementację oraz dodatkowe 6 na określenie dostawców kluczowych usług w jej rozumieniu. Okres ten upływa odpowiednio w 9 maja 2018 roku i 9 listopada 2018 roku. W Polsce prace nad projektem ustawy wprowadzającej Dyrektywę NIS, tj. ustawy o krajowym systemie cyberbezpieczeństwa prowadzi Ministerstwo Cyfryzacji. Projekt tej ustawy ma zostać opublikowany w kwietniu 2017 roku.

I. PREAMBUŁA DYREKTYWY NIS.

1. Dyrektywa została przyjęta ze względu na fakt, że incydenty w zakresie bezpieczeństwa stanowią co raz większe zagrożenie dla funkcjonowania sieci i systemów informatycznych. Systemy te mogą się również stać obiektem umyślnych szkodliwych działań, mających na celu uszkodzenie lub przerwanie ich działania. Tego typu incydenty mogą utrudniać prowadzenie działalności gospodarczej, powodować znaczne straty finansowe, podważać zaufanie użytkowników oraz powodować poważne straty w gospodarce Unii.

Podkreślono również, że obecne zdolności Państw Członkowskich nie są wystarczające dla zapewnienia wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych w Unii oraz, że poziom ten różni się znacząco pomiędzy poszczególnymi Państwami Członkowskimi.

2. Jednym z założeń Dyrektywy NIS jest powołanie do życia grupy współpracy na wypadek kryzysów w cyberprzestrzeni (dalej: Grupa Współpracy), w skład której mają wchodzić m. in. przedstawiciele Państw Członkowskich. Grupa Współpracy ma propagować i proponować rozwiązania zapewniające odpowiedni poziom zabezpieczeń w systemach informatycznych. W skład Grupy Współpracy ma wchodzić Agencja UE ds. Bezpieczeństwa Sieci i Informacji (ENISA).

3. Dyrektywa NIS ma znaleźć zastosowanie do operatorów usług kluczowych i dostawców usług cyfrowych, wskazanych w załącznikach do niej. Państwom Członkowskim pozostawiono określenie, które podmioty należą do tych kategorii, w oparciu o wytyczne zawarte w Dyrektywie NIS. Określenie tych dostawców następuje w oparciu o kryterium sektora gospodarki, w którym operują.

4. W Dyrektywie NIS dostrzeżono wzrost znaczenia usług „chmurowych”.

5. Dostawcy usług cyfrowych mają zapewniać poziom bezpieczeństwa współmierny do stopnia ryzyka, na jakie narażone jest bezpieczeństwo świadczonych przez nich usług cyfrowych.

6. Operatorzy usług kluczowych i dostawcy usług cyfrowych mają zapewniać bezpieczeństwo sieci i systemów informatycznych, których używają.

7. Wymogi w zakresie zapewnienia cyberbezpieczeństwa mają uwzględniać najnowszy stan wiedzy na temat takich środków.

8. Administracje publiczne Państw Członkowskich muszą mieć zapewnioną możliwość stawiania dodatkowych wymogów dostawcom usług, w szczególności w zakresie usług chmurowych.

9. Dyrektywa NIS podkreśla znaczenie bezpieczeństwa usług przetwarzania w chmurze, w szczególności świadczonych na rzecz sektora publicznego. Wskazano m. in., że Dyrektywa NIS nie powinna uniemożliwiać państwom członkowskim przyjmowania środków krajowych zobowiązujących podmioty sektora publicznego do zapewnienia szczególnych wymogów w zakresie bezpieczeństwa, w przypadku gdy zawierają one umowy na usługi przetwarzania w chmurze.

10. Wskazano również, że w wielu przypadkach incydentów bezpieczeństwa istnieje ryzyko naruszenia danych osobowych. W tym kontekście właściwe organy oraz organy ochrony danych powinny ze sobą współpracować oraz wymieniać się informacjami dotyczącymi wszystkich istotnych kwestii w celu rozwiazywania problemów związanych z wszelkimi przypadkami naruszeń danych osobowych w wyniku incydentów.

11. Zadanie określenia procedur funkcjonowania Grupy Współpracy, wymogów dotyczących bezpieczeństwa oraz procedury zgłaszania incydentów bezpieczeństwa powierzono Komisji Europejskiej, która ma wydać akty wykonawcze.

II. POSTANOWIENIA DYREKTYWY NIS.

1. Dyrektywa NIS ustanawia obowiązek przyjęcia krajowych strategii w zakresie bezpieczeństwa sieci i systemów informatycznych.

2. Dyrektywa NIS tworzy Grupę Współpracy.

3. Tworzy sieć zespołów reagowania na incydenty bezpieczeństwa komputerowego.

4. Dyrektywa NIS zobowiązuje Państwa Członkowskie do zidentyfikowania operatorów usług kluczowych, według kryterium sektorów i podsektorów wskazanych w załączniku do tej dyrektywy.

Wymieniono 7 sektorów: energetyka, transport, bankowość, infrastruktura rynków finansowych, służba zdrowia, zaopatrzenie w wodę pitną i jej dystrybucja oraz infrastruktura cyfrowa. W każdym z tych sektorów Państwo Członkowskie ma obowiązek wskazać operatorów usług kluczowych do dnia 9 listopada 2018 roku.

5. Dyrektywa NIS reguluje świadczenie usług cyfrowych. W załączniku nr 3 do tej dyrektywy wymieniono 3 rodzaje usług, których ona dotyczy, to jest internetową platformę handlową, wyszukiwarkę internetową oraz usługę przetwarzania w chmurze.

6. Każde Państwo Członkowskie ma obowiązek wprowadzenia krajowej strategii w zakresie bezpieczeństwa sieci i systemów informatycznych. Strategia ta ma doprowadzić do zapewnienia odpowiedniego poziomu ochrony na incydenty bezpieczeństwa w cyberprzestrzeni.

7. Każde Państwo Członkowskie wyznacza co najmniej jeden organ krajowy ds. Bezpieczeństwa sieci i systemów informatycznych, który monitoruje stosowanie Dyrektywy NIS na poziomie krajowym.

8. Każde Państwo Członkowskie wyznacza zespół reagowania na incydenty bezpieczeństwa komputerowego.

9. Państwa Członkowskie zapewniają, aby operatorzy usług kluczowych podejmowali odpowiednie i proporcjonalne środki techniczne i organizacyjne w celu zarzadzania ryzykami, na jakie narażone są wykorzystywane przez nich sieci i systemy informatyczne. Uwzględniając najnowszy stan wiedzy, środki te muszą zapewniać poziom bezpieczeństwa sieci i systemów informatycznych odpowiedni do istniejącego ryzyka.

10. Państwa Członkowskie zapewniają, aby operatorzy usług kluczowych podejmowali odpowiednie środki zapobiegające i minimalizujące wpływ incydentów dotyczących bezpieczeństwa sieci i systemów informatycznych wykorzystywanych w celu świadczenia takich usług kluczowych, z myślą o zapewnieniu ciągłości tych usług.

11. Państwa członkowskie zapewniają, aby właściwe organy miały uprawnienia i środki niezbędne do oceny wypełniania przez operatorów usług kluczowych ich obowiązków oraz jego skutków dla bezpieczeństwa sieci i systemów informatycznych.

12. Państwa Członkowskie zapewniają, aby właściwe organy miały uprawnienia i środki, pozwalające wymagać od operatorów usług kluczowych przekazywania niezbędnych informacji oraz dowodów dotyczących zapewnienia środków ochrony.

13. Państwa Członkowskie zapewniają, aby właściwy organ mógł wydać operatorom usług kluczowych wiążące polecenia wprowadzenia środków zaradczych w odniesieniu do stwierdzonych uchybień.

14. Obsługując incydenty, które doprowadziły do naruszeń danych osobowych, właściwy organ działa w ścisłej współpracy z organami ochrony danych.

15. Państwa członkowskie zapewniają, aby dostawcy usług cyfrowych określali i podejmowali odpowiednie i proporcjonalne środki techniczne i organizacyjne w celu zarządzania ryzykami, na jakie narażone są sieci i systemy informatyczne wykorzystywane przez nich w kontekście oferowania usług na terenie w UE. Uwzględniając najnowszy stan wiedzy, środki te muszą zapewniać poziom bezpieczeństwa sieci i systemów informatycznych odpowiedni do istniejącego ryzyka oraz uwzględniać następujące elementy: a) bezpieczeństwo systemów i obiektów; b) postepowanie w przypadku incydentu; c) zarzadzanie ciągłością działania; d) monitorowanie, audyt i testowanie; e) zgodność z normami międzynarodowymi.

16. Państwa członkowskie zapewniają, aby właściwe organy podjęły działania, w razie konieczności, w drodze środków nadzorczych *ex post*, gdy otrzymają dowód, że dostawca usług cyfrowych nie spełnia wymogów określonych w Dyrektywie NIS. Taki dowód może zostać przekazany przez właściwy organ innego państwa członkowskiego, w którym usługa jest świadczona.

17. Do tych celów właściwe organy muszą mieć uprawnienia i środki niezbędne do wymagania od dostawców usług cyfrowych przekazywania informacji niezbędnych do oceny bezpieczeństwa ich sieci i systemów informatycznych, w tym dokumentów dotyczących polityki w zakresie bezpieczeństwa oraz eliminowania wszelkich przypadków niespełnienia wymogów określonych w Dyrektywie NIS. Dotyczy to m. in. dostawców usług chmurowych.