
fot. unsplash.com

Ireneusz Piecuch,
Senior Partner, DGTL Kibil Piecuch i Wspólnicy S.K.A.

NIS - reaktywacja

Kiedy cztery lata temu pojawiła się dyrektywa 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"), wydawało się, że zostanie z nami na dłużej. Adresowała przecież obszar, który nie był do tego momentu przedmiotem żadnej spójnej regulacji, a wiadomym było, że w niektórych krajach (między innymi w Polsce), jej implementacja oznacza stworzenie zupełnie nowej dziedziny prawa.

To zaś nie dzieje się z dnia na dzień. Większość krajów faktycznie uchwaliła przepisy implementujące Dyrektywę NIS do prawa krajowego w zakładanym terminie, czyli do 10 maja 2018 r. Jeżeli chodzi jednak o proces wdrożenia tych postanowień, to tu zaczęły się schody. W Polsce, która zaimplementowała bardzo rozbudowany model administracji obszarem cyberbezpieczeństwa, praktycznie do czasów obecnych nie wydano jeszcze wszystkich decyzji o wyznaczeniu operatorów usług krytycznych. Warto wspomnieć, że nie przeszkodziło to nam dopracować się ostatnio projektu zmiany tej ustawy, który ten układ dodatkowo skomplikuje. Jak jednak widać, zakusy wprowadzania ulepszeń do regulacji nie są wyłącznie naszą specjalnością. Komisja Europejska analizując obecny stan systemu regulacji w zakresie cyberbezpieczeństwa, doszła do wniosku, że zmiany są niezbędne. I to zmiany w takim zakresie, że konieczne będzie uchwalenie zupełnie nowej dyrektywy. Tu i ówdzie pojawiały się nawet poglądy, że może tak wzorem RODO warto byłoby się pokusić o rozporządzenie, ale pomysł ten nigdy się nie skrystalizował. Należy pamiętać, że rozporządzenie w sprawie ochrony danych osobowych, było wprowadzone po kilkunastu latach obowiązywania poprzedzającej je dyrektywy, która obowiązując wiele lat, na dobre zadomowiła się w systemach państw członkowskich. Było na czym budować. W przypadku Dyrektywy NIS nie ma mowy o porównywalnym doświadczeniu, stąd w propozycji jedynie zmiana treści, ale nie rodzaju aktu prawnego. Dlaczego zmian okazała się konieczna?

Wiele elementów nie działa. Jak działają, to na ogół źle, a jeśli działają dobrze - to nie przynoszą oczekiwanych rezultatów

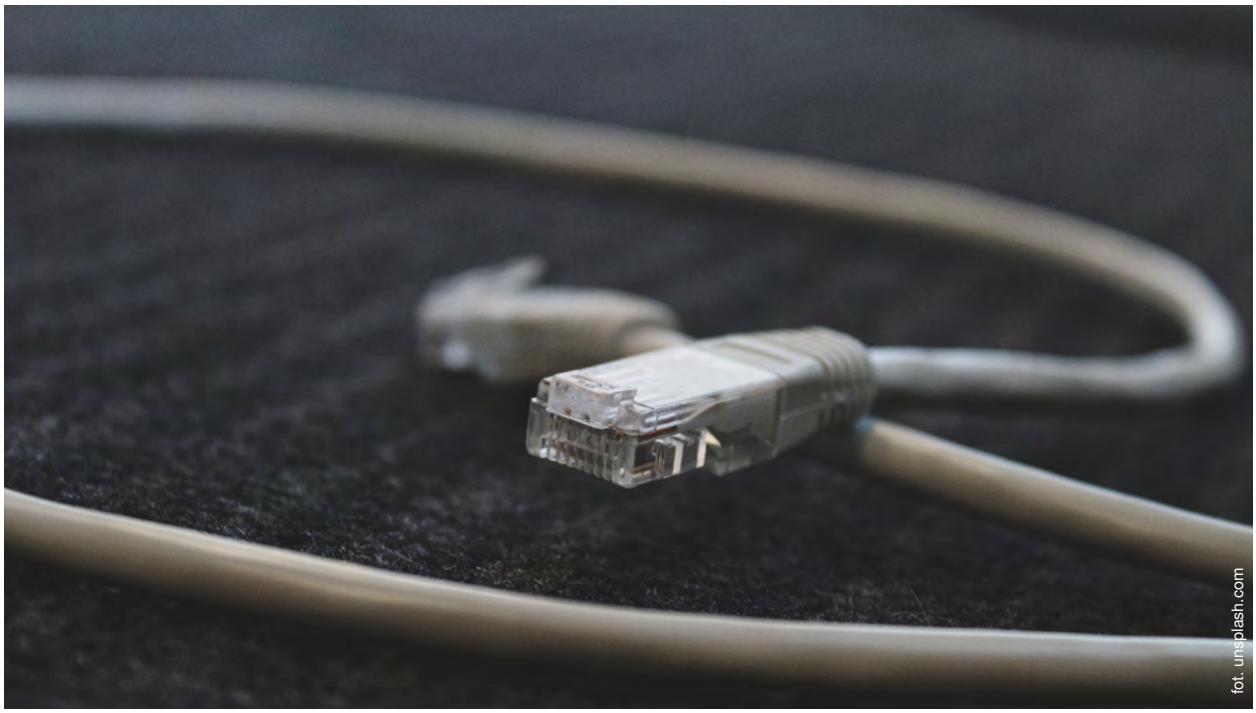
Zdaniem KE Dyrektywa NIS I objęła zbyt wąską grupę przedsiębiorstw, a to z uwagi na to, że stopień usieciowienia i cyfryzacji przekroczył znacznie zakładane wcześniej wielkości. Skutkiem czego pojawiły się obszary kluczowe dla rozwoju cyfrowej gospodarki europejskiej, pozostające poza zasięgiem oddziaływania dyrektywy. Gdyby był to jedyny problem, wystarczyłaby zapewne korekta obecnie obowiązującej dyrektyw. Ale tak nie jest. Zdaniem Komisji, rozwiązaniom przyjętym w NIS I brakowało wystarczającej precyzji, skutkiem czego określone grupy przedsiębiorstw były regulowane w kilku krajach, a w kilku innych już nie (przykładowo szpitale). Rozjechały się także systemy raportowania przyjmowane przez poszczególne państwa europejskie, co utrudniało, a czasami uniemożliwiało efektywne zarządzenie wyzwaniem cyberzagrożeń w skali europejskiej. Do tego doszedł nieefektywny nadzór i brak odpowiednio sprawnej egzekucji, olbrzymie zróżnicowanie w nakładach na zasoby ludzkie i budżetowe przypisane do realizacji zadań opisanych w NIS I i brak systematycznego współdzielenia informacji pomiędzy państwami UE. Patrząc na wyliczankę Komisji, aż chciałoby się zapytać: to co w końcu zadziałało?

Faktycznie.

W mieście pojawi się nowy szeryf … z licencją na zamykanie

Czytając projekt NIS II widać zupełnie inne podejście do niektórych kwestii. I może warto zacząć od końca. Wszyscy recenzenci Dyrektywy NIS I, byli zgodni, że w kwestiach egzekucji naruszeń i sankcji z tym związanych, dyrektywa ta była niezwykle lakoniczna. Skutek, był taki, że w Polsce najwyższą możliwą karą do nałożenia za naruszenie ustawy była kara jednego mln złotych. Biorąc pod uwagę fakt, że polska ustawa o krajowym systemie bezpieczeństwa wchodziła w życie mniej więcej w tym samym czasie, kiedy przedsiębiorcy mierzyli się z wyzwaniami RODO oraz drakońskimi karami przewidzianymi w tym rozporządzeniu, niewielu było takich, którzy wierzyli w możliwość sprawnego wdrożenia ustawy pozbawionej realnych sankcji. Według projektu NIS II, element ten ulegnie diametralnej zmianie. I to nie dlatego, że maximum kary wzrośnie do 10 mln Euro (czyli prawie czterdzieści pięć razy), albo 2% łącznego rocznego obrotu uzyskanego na całym świecie, ale dlatego, że zgodnie z projektem nowej dyrektywy państwa członkowskie będą musiały wprowadzić szereg mechanizmów zwiększających prawdopodobieństwo przestrzegania nowych przepisów.

Czego zatem mogą spodziewać się przedsiębiorcy podlegający nowym przepisom po implementacji NIS II? Inspekcji w swojej siedzibie, nadzoru nad działaniami prowadzonymi on-line, losowych weryfikacji. Oprócz obowiązków przeprowadzania standardowych audytów pojawią się audyty celowe związane z oceną ryzyka. Konieczność dostarczania określonej dokumentacji na życzenie uprawnionych organów. Konieczność udzielania dostępu do danych, jeśli jest to konieczne dla sprawowania nadzoru. 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. Ostrzeżenie jest najłagodniejszym z nich. Kolejnym jest wiążąca instrukcja lub nakaz dotyczący usunięcia zidentyfikowanych niezgodności lub naruszeń obowiązków przewidzianych w NIS II. Nakaz podjęcia określonych działań w zakresie zarządzania ryzykiem - w określony sposób i w określonym czasie. Nakaz poinformowania osób, na rzecz których przedsiębiorca świadczy usługi o grożącym im zagrożeniu i istniejących możliwościach podjęcia przez takie osoby konkretnych działań mających na celu zaadresowanie tych ryzyk. Nakaz wdrożenia zaleceń audytu w określonym terminie. Regulator będzie też mógł delegować swojego pracownika do nadzorowania (w określonym czasie) wskazanych działań w zakresie wprowadzania obowiązków przewidzianych w NIS II oraz podawać do publicznej wiadomości nazwy przedsiębiorców,


fot. unsplash.com

którzy dopuścili się naruszeń Dyrektywy oraz rodzaju tych naruszeń. A także ... a jakże, nakładać kary. Do tego dochodzi możliwość zawieszenia autoryzacji lub certyfikacji określonych usług i zawieszania w obowiązkach osób z kierownictwa firmy dopuszczającej się naruszeń.

Kluczowe, Ważne i ... Małe też

NIS II utrzyma kategorię operatorów usług krytycznych, ale znika kategoria dostawców cyfrowych, których obowiązki w NIS I kształtowane były nieco odmiennie. Zamiast dostawców usług cyfrowych pojawi się druga kategoria operatorów usług istotnych, w skład której wejdą m. in.: firmy pocztowe i kurierskie, firmy składujące i przetwarzające odpady, wytwórcy, producenci oraz dystrybutorzy chemikaliów, producenci i dystrybutorzy żywności, producenci przemysłowi oraz dostawcy cyfrowi). Mikro oraz mali przedsiębiorcy (przedsiębiorcy zatrudniający do 50 osób, których roczny bilans nie przekracza 10 mln Euro), będą z ustawy wyłączeni, chyba, że stosować się będzie do nich jeden z wyjątków opisanych w NIS II. Przykładowo tacy, w przypadku których naruszenie świadczonych przez nich usług mogłoby mieć wpływ na bezpieczeństwo publiczne, albo zdrowie publiczne. Dość pojemny wyjątek - jeden z siedmiu.

Innymi słowy, uprawnionym jest przypuszczenie, że liczba podmiotów podlegających NIS II ulegnie istotnemu przyrostowi. Z jednej strony to dobrze, bo oprogramowanie złośliwe nie rozróżnia wielkości przedsiębiorstwa podczas ataku. Z drugiej jednak strony wychodzi na to, że wiele przedsiębiorstw nie objętych obecnie obowiązkami KSC, będzie musiało poważnie przemyśleć swoje podejście do zagadnienia cyberbezpieczeństwa. Dwa omówione wyżej obszary, nie stanowią pełnej listy proponowanych zmian. W NIS II znalazł się jeszcze zapis o możliwości nakładania przez państwa członkowskie wymogów stosowania określonych norm europejskich, co było postulowane od dawna przez wielu specjalistów. Znalazły się zapisy odnośnie koordynacji działań w zakresie oceny ryzyka związanego z określonymi łańcuchami dostaw, czego przedsmak mieliśmy już przy okazji analizy ryzyka związanego z dostawami elementów dla sieci 5G. Mamy też, co o dziwo może okazać się bardzo dobrym i praktycznym rozwiązaniem, obowiązek przechodzenia szkoleń z zakresu cyberbezpieczeństwa przez osoby zarządzające przedsiębiorcami.

Oczywiście od projektu do implementacji do porządku krajowego dzielą nas jeszcze mniej więcej dwa lata. Ale należy pamiętać, że poprzednia dyrektywa była dość pojemna i wiele elementów z propozycji NIS II może być wdrożone już teraz, bez czekania na uchwalenie dyrektywy i wejście jej w życie. Z drugiej strony, może pojawić się pytanie: czy za dwa lata, tak zmieniona dyrektywa będzie w dalszym ciągu adekwatna do poziomu ówczesnego poziomu rozwoju cyfrowej gospodarki? Kilka kwestii wydaje się jednak pewne. Zmiany nadchodzą. Kary ulegną zwiększeniu i będą nakładane tak jak ma to miejsce w przypadku RODO. Regulator dostanie daleko idące uprawnienia. A cyberprzestępcy nie zrezygnują z bajecznego interesu. Warto więc zacząć patrzeć na nakłady na cyberbezpieczeństwo nie jako na koszt (co obecnie dominuje), tylko jako na inwestycję w ochronę przychodów. □