DYREKTYWA NIS: GŁÓWNE ZMIANY ORAZ NAJWIĘKSZE PROBLEMY [ANALIZA]

Organizacja i funkcjonowanie wielu państwowych i prywatnych podmiotów z sektorów energetycznego, transportowego, bankowości i infrastruktury rynków finansowych, służby zdrowia, zaopatrzenia w wodę oraz infrastruktury cyfrowej oparte są na systemach informatycznych i co za tym idzie wiąże się to z ryzykiem wystąpienia incydentów związanych z ich bezpieczeństwem. Każde takie zaburzenie może w istotny sposób odbić się nie tylko na gospodarce danego państwa członkowskiego ale także na całej gospodarce UE.

Od sierpnia 2016 roku obowiązuje dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 *w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii* zwana Dyrektywą NIS. Analizując dokumenty rządowe daje się zauważyć, że polskie władze pokładają wielkie nadzieje w rozwiązaniach przewidzianych przez powyższy akt. W Krajowych Ramach Polityki Cyberbezpieczeństwa RP na lata 2017- 2022 rząd stawia na walkę z dystrybucją szkodliwego oprogramowania, włamaniami do systemów teleinformatycznych czy blokowaniem możliwości świadczenia usług. Cel wprowadzonych zmian jest ambitny – chodzi bowiem o zapewnienie wysokiego poziomu odporności krajowych systemów teleinformatycznych, operatorów kluczowych usług i dostawców usług cyfrowych (internetowych platform handlowych, wyszukiwarek internetowych i usług przetwarzania w chmurze) na ataki w cyberprzestrzeni.

Powyższe cele mają zostać zrealizowane poprzez wdrożenie instrumentów przewidzianych w Dyrektywie NIS. Wymaga ona bowiem, aby każde państwo członkowskie sporządziło wykaz usług kluczowych, umożliwiający jednocześnie identyfikacje operatorów usług kluczowych. Celem wykazu jest więc identyfikacja zarówno rodzajów usług kluczowych jak również operatorów usług kluczowych. Nie jest do końca jasne, które podmioty mają zostać objęte odpowiednimi regulacjami. Ta wątpliwość jest tym bardziej istotna z uwagi na istniejący już wykaz infrastruktury krytycznej RP. Problemem może się okazać określenie wzajemnych relacji pomiędzy tymi dokumentami.

Jeśli chodzi o dostawców usług cyfrowych, od których zależnych jest wielu przedsiębiorców, z uwagi na zakładany przez unijnego prawodawcę - mniejszy stopień ryzyka wystąpienia incydentu - wymogi w zakresie bezpieczeństwa są znacznie mniejsze. W związku z tym, wdrożone przez przyszłą Polską ustawę instrumenty prawne muszą pozostawić tym dostawcom swobodę podejmowania środków, które sami uznają za odpowiednie do zarządzania ryzykami, na jakie może być narażone bezpieczeństwo ich sieci i systemów informatycznych.

W przeciwieństwie do operatorów usług kluczowych, w przypadku dostawców usług cyfrowych Polska nie będzie miała obowiązku ich identyfikacji. Z uwagi na transgraniczny charakter działalności takich usługodawców Dyrektywa NIS będzie miała zastosowanie do wszystkich dostawców usług cyfrowych. Z uwagi na tę „transgraniczność" Dyrektywa NIS przewiduje konieczność zwiększonej harmonizacji w odniesieniu do wymogów zakresie bezpieczeństwa i zgłaszania incydentów.

Czytaj też: [Dyrektywa NIS przyjęta – co to oznacza dla cyberbezpieczeństwa Polski i Europy?]

Założeniem jest, że dostawcy usług cyfrowych powinni podlegać łagodnym działaniom nadzorczym, uruchamianym dopiero w przypadku istnienia realnego dowodu na to, że nie spełniają oni wymogów dotyczących bezpieczeństwa. W ich przypadku nie może być mowy o istnieniu ogólnego obowiązku nadzorczego.

Polska ustawa powinna uzależniać wymogi w zakresie bezpieczeństwa od ryzyka związanego z daną siecią oraz danym systemem informatycznym. Wobec tego, celem uniknięcia sytuacji, w której dojdzie do nałożenia na operatorów usług kluczowych i dostawców usług cyfrowych wysokich wymagań, pociągających za sobą wysokie koszty finansowe i obciążenia administracyjne, wymogi te powinny być proporcjonalne do ryzyka związanego z daną siecią. W zakresie usług kluczowych Polska może nałożyć na odpowiednich operatorów bardziej rygorystyczne wymogi, od tych przewidzianych w Dyrektywie NIS. Jeśli zaś chodzi o dostawców usług cyfrowych, wymogi te nie powinny mieć zastosowania ani do mikroprzedsiębiorstw ani też do małych przedsiębiorstw.

Sens Dyrektywy NIS sprowadza się do stworzenia skutecznego systemu, w którym operatorzy usług kluczowych będą posiadali właściwe środki do realizacji celu w postaci zarządzania ryzykami, na jakie narażone są wykorzystywane przez nich sieci i systemy informatyczne. Środki te powinny jednocześnie zapobiegać i minimalizować wpływ incydentów dotyczących bezpieczeństwa sieci. Skutecznej organizacji środków bezpieczeństwa ma służyć obowiązkowy system notyfikacji incydentów mających istotny wpływ na ciągłość świadczonych przez nich usług kluczowych.

Wdrożenie odpowiednich środków bezpieczeństwa a także informowanie o zaistniałych incydentach to podstawowe obowiązki, z którymi będą musiały zmierzyć się podmioty objęte zakresem Dyrektywy NIS. W zakresie tego drugiego obowiązku, problemem może okazać się kwestia zdecydowania o tym, czy dany incydent będzie miał istotny wpływ na ciągłość świadczonych przez te podmioty usług kluczowych. Dyrektywa NIS nakazuje, aby przy ocenie wagi, znaczenia oraz zasięgu danego incydentu kierować się następującymi kryteriami: (I) liczbą użytkowników, których dotyczy zakłócenie usługi kluczowej; (II) czasem trwania incydentu; (III) zasięgiem geograficznym związanym z obszarem, którego dotyczy incydent.

Podmioty objęte Dyrektywą NIS będą musiały niezwłocznie (operatorzy usług kluczowych) lub bez zbędnej zwłoki (dostawcy usług cyfrowych) zgłaszać właściwemu organowi lub CSRIT incydenty związane z bezpieczeństwem. Ustawodawca Polski będzie musiał jasno określić, w jakim konkretnie terminie i jakiemu konkretnie organowi owe incydenty zobowiązane podmioty będą musiały zgłaszać. Niemałym problemem może okazać się także ustalenie, jakie konkretnie informacje, powinny znaleźć się w zgłoszeniu o incydencie.

W maju 2018 roku Polsce upłynie termin na implementacje Dyrektywy NIS. Do tego dnia wszystkie przepisy zarówno ustawowe jak i wykonawcze do ustawy muszą być przez Polskę przyjęte i ogłoszone. Z kolei z początkiem listopada 2018 r. w odniesieniu do każdego sektora i podsektora objętego zakresem Dyrektywy NIS, Polska ma obowiązek dokonać identyfikacji operatorów usług kluczowych posiadających jednostkę organizacyjną na jej terytorium. Problemów związanych z implementacją jest więc sporo a czas cały czas biegnie.

Magdalena Wicha – aplikant adwokacki w Kancelarii Prawniczej Kruk i Wspólnicy