Cyberbezpieczeństwo – modny slogan czy realny problem dla energetyki?

Nadszedł czas, kiedy cyberbezpieczeństwo doczekało się kompleksowej regulacji prawnej. Nowe przepisy implementujące unijną dyrektywę NIS weszły w Polsce w życie 28 sierpnia 2018 r. Nie dla wszystkich jest jednak jasne, czy i w jakim zakresie dotyczą ich nowe obowiązki. Ustawa wyróżnia trzy kategorie podmiotów, które muszą dostosować swoją działalność do nowych regulacji – operatorów usług kluczowych, dostawców usług cyfrowych oraz podmioty publiczne. Zadanie jakie przed nimi stoi nie jest proste, a czas na dostosowanie patrząc przez pryzmat ilości obowiązków – bardzo krótki.

Sektor energia został zakwalifikowany jako jeden z sześciu obszarów działalności kluczowych z punktu widzenia krajowego systemu cyberbezpieczeństwa. W jego ramach wyróżniono siedem podsektorów – wydobycie kopalin, energia elektryczna, ciepło, ropa naftowa, gaz oraz dwa wydzielone funkcjonalnie, tj. dostawy i usługi dla sektora energii oraz jednostki nadzorowane i podległe Ministrowi Energii. Oznacza to, że praktycznie wszystkie przedsiębiorstwa prowadzące działalność energetyczną muszą zweryfikować czy i w jakim zakresie podlegają pod nowe przepisy oraz zidentyfikować jakie ich działania mieszczą się w definicji usługi kluczowej lub zadania publicznego. Uzyskanie statusu operatora usługi kluczowej albo zakwalifikowanie jako podmiot publiczny ma istotne konsekwencje – powoduje włączenie przedsiębiorstwa do krajowego systemu cyberbezpieczeństwa.

Kto będzie operatorem usługi kluczowej?

Kwalifikacji poszczególnych podmiotów jako operatorów usługi kluczowej nie odbywa się automatycznie. Przepisy uzyskanie tego statusu uzależniają od otrzymania decyzji administracyjnej. Obowiązek zweryfikowania kto spełnia ustawowe wymogi został nałożony na organy właściwe do spraw cyberbezpieczeństwa. W przypadku sektora energia jest to Minister Energii. Właśnie ten organ musi zweryfikować czy są podstawy do wydania decyzji o uznaniu za operatora usługi kluczowej w stosunku do poszczególnych przedsiębiorstw energetycznych. Wiele firm ma już tego świadomość, ponieważ otrzymało do wypełnienia ankiety dotyczące ich działalności w obszarach zakwalifikowanych jako usługi kluczowe, które stanowią bazę do weryfikacji prowadzonej przez Ministra Energii.

Biorąc pod uwagę ustawowe kryteria kwalifikacji, decyzji mogą spodziewać się nie tylko najwięksi rynkowi gracze. **Za operatorów usługi kluczowej może zostać uznanych wiele OSDn.** Ustalony w przepisach próg kwalifikujący do uzyskania statusu operatora usługi kluczowej w obszarze dystrybucji energii elektrycznej powoduje, że w skład krajowego systemu cyberbezpieczeństwa mogą wejść przedsiębiorstwa prowadzące działalność na naprawdę niewielką skalę. **Drugą grupą szczególnie liczną grupą operatorów usług kluczowych będą przedsiębiorstwa ciepłownicze. Dotyczy to zarówno wytwarzania jak i zaopatrywania odbiorców w ciepło.** Kryteria dla tego

podsektora zostały sformułowane w sposób budzący sporo wątpliwości interpretacyjnych, jednak już teraz wiadomo, że skala działalności nie musi być bardzo duża. W uproszczeniu można przyjąć, że wszystkie te przedsiębiorstwa, które zaopatrują w ciepło odbiorców końcowych w miastach zamieszkanych przez co najmniej 15 tysięcy odbiorców powinny zweryfikować, czy cyberbezpieczeństwo będzie też ich dotyczyć.

Portfolio usług kluczowych może być szerokie

Dla niektórych podmiotów sporym zaskoczeniem jest, że mogą być operatorem usług kluczowych w kilku obszarach. Najczęściej dotyczy to łączenia działalności energetycznej, wodno-kanalizacyjnej i transportowej. Często zdarza się, że jedna firma zajmuje się działaniami w kilku obszarach, a szczególnie o działalności energetycznej często się zapomina. Fakt, że nie stanowi ona podstawowej działalności przedsiębiorstwa nie powoduje wyłączenia go spod nowych przepisów. Z punktu widzenia tych regulacji znaczenie ma to, czy przedsiębiorstwo faktycznie wykonuje usługę, która znajduje się w wykazie usług kluczowych, a nie to jak ocenia jej istotność z punktu widzenia swojej działalności. Oznacza to, że jedna firma może otrzymać decyzje od różnych organów do spraw cyberbezpieczeństwa. Dlatego mówiąc sektor energia rozumie się szeroki krąg podmiotów.

Podmiot (nie)publiczny też musi się przygotować

Przedsiębiorstwo energetyczne może nie spełniać progów, które zakwalifikowałyby je jako operatora usługi kluczowej. Nie oznacza to jednak, że może zapomnieć o nowych wymaganiach. **Podmiotem publicznym w rozumieniu przepisów o krajowym systemie cyberbezpieczeństwa są również przedsiębiorstwa działające w sektorze prywatnym**. W tej kategorii znajdują się więc nie tylko jednostki samorządu terytorialnego, ale również spółki, które realizują zadania publiczne. Pojęcie zadania publicznego jest stosunkowo szerokie i w dużym zakresie obejmuje działalność energetyczną. Dotyczy to w szczególności dostarczania ciepła i oświetlenia w gminach, ale nie wyłącznie. Każdy przypadek jest indywidualny, dlatego przedsiębiorstwa które nie będą miały statusu operatora usługi kluczowej, muszą sprawdzić, czy nie kwalifikują się do krajowego systemu cyberbezpieczeństwa jako podmioty publiczne i ustalić swoje obowiązki przez pryzmat tego statusu.

Zapewnienie cyberbezpieczeństwa nie zawsze wygląda tak samo

Przedsiębiorstwa energetyczne żeby wiedzieć, czemu stawiają czoła w związku z przepisami o cyberbezpieczeństwie muszą w pierwszej kolejności ustalić swój statusu na gruncie tych regulacji. Dopiero wówczas możliwe jest ustalenie zakresu ich nowych obowiązków. W przypadku operatorów usług kluczowych wymagany od nich poziom bezpieczeństwa jest stosunkowo wysoki. Podmioty, które uzyskają ten status będą musiały wdrożyć u siebie kompleksowy system zarządzania bezpieczeństwem w systemach, które wykorzystują do świadczenia usługi kluczowej. Oznacza to konieczność zapewnienia odpowiedniego sposobu eksploatacji tych systemów i stosowania odpowiednich procedur dotyczących pracy z nimi. Bezpieczeństwo to

również odpowiednie zabezpieczenia techniczne oraz system identyfikowania podatności i zarządzania incydentami. Zakres nowych obowiązków nałożonych na podmioty publiczne jest mniejszy niż w przypadku operatorów usług kluczowych, jednak i w ich przypadku dostosowanie się do nowych realiów może być sporym wyzwaniem. Kluczowym aspektem dla osiągnięcia zgodności z przepisami o cyberbezpieczeństwie jest właściwa identyfikacja ryzyk związanych z korzystaniem z systemów informacyjnych. Bez tego nie można mówić o skutecznych zabezpieczeniach czy dobrze przygotowanych procedurach.

Jak uniknąć powtórki z RODO

Realnym problemem dla całego rynku na pewno jest to, że nie wszystkie firmy mają rozbudowane działy IT, a o specjalistów na rynku może być coraz trudniej. Nie chodzi tutaj jednak wyłącznie o ograniczenia organizacyjne. Dostosowanie się do nowych wymogów to przede wszystkim wyzwanie związane z ustaleniem tego, jak znaleźć złoty środek miedzy bezpieczeństwem a optymalizacją kosztów. W szczególności w przypadku podmiotów publicznych. Z punktu widzenia kosztów, które wiążą się z zapewnieniem compliance w obszarze cyberbepieczeństwa prowadzonej działalności tylko wczesne zidentyfikowanie planu działania. Ratunkiem może być oczywiście zlecenie tych działań na zewnątrz. Jednak przy wybieraniu dostawców usług jedynie w oparciu o kryterium ceny można mieć wątpliwość, czy cyberbezpieczeństwo będzie mogło funkcjonować w praktyce czy tylko na papierze. Te doświadczenia są już zresztą dobrze znane na rynku po przejściu przez dostosowanie do przepisów RODO. Dlatego kluczowe powinno być doświadczenie i znajomość specyfiki branży. Błędy na etapie ustalania obowiązków czy wycinkowe wprowadzanie zmian mogą okazać się problemem później. Dostosowanie do nowych przepisów nie może też być tylko na papierze. Incydentom w systemach, bez względu na to czy wynikają z błędów ludzkich czy ataków hakerskich, nie przeciwdziała się tylko papierem.

Wdrożenie cyberbezpieczeństwo musi zawsze poprzedzić inwentaryzacja systemów

Z przepisów wynika, że cyberbezpieczeństwo to odporność systemów informacyjnych w zakresie w jakim przetwarzają dane lub są wykorzystywane do realizacji usług kluczowych. System informacyjny do świadczenia usługi kluczowej to nie musi być każde oprogramowanie, jakie działa w firmie. Zgodnie z ustawową definicją system informacyjny jest rozumiany jako system teleinformatyczny, a więc w dużym uproszczeniu - współpracujące ze sobą urządzenia i oprogramowanie, które są wykorzystywane do przetwarzania, przechowywania i transferu danych przez sieci telekomunikacyjne. Kluczowa jest jednak odpowiedź na pytanie, co to oznacza w praktyce.

Wątpliwości można mieć sporo. Po pierwsze pojawia się pytanie jakie systemy mają status systemów informacyjnych. Ze względu na postęp technologiczny zakres urządzeń, które przetwarzają i przesyłają między sobą dane jest coraz większy. Poszczególne maszyny komunikują się ze sobą przesyłając określone dane. Operator usługi kluczowej musi prześledzić strukturę swojej sieci i ustalić, które systemy mają określone w przepisach

właściwości i są związane z realizacją usług określonych jako kluczowe. Wątpliwości mogą budzić w szczególności te aplikacje lub programy, które służą do zarządzania procesami organizacyjnymi. Dodatkowo rozstrzygnięcie, które procesy przetwarzania dotyczą usług kluczowych może wcale nie być proste.

Cyberbezpieczństwo wymaga wdrożenia odpowiednich procedur i dokumentów

Przepisy formułują minimalne standardy dotyczące cyberbezpieczeństwa. Jednak to przedsiębiorstwo energetyczne będzie musiało zweryfikować, czy funkcjonujący w nim system zarządzania bezpieczeństwem informacji jest właściwy. Nie dla wszystkich na rynku będzie się to wiązało z rewolucją. Te przedsiębiorstwa u których funkcjonują już określone rozwiązania i odpowiednia dokumentacja cyberbezpieczeństwa, będą mogły myśleć raczej o ewolucji istniejących rozwiązań. Tematyka compliance jest jednak znacznie szersza niż tylko cyberbezpieczeństwo. Wymaga uwzględnienia kwestii związanych z przetwarzaniem danych osobowych czy innych wymogów dotyczących specyfiki danego systemu. Tworzenie struktur odpowiedzialnych za cyberbezpieczeństwo wymaga dokumentów i procedur sformułowanych zgodnie z przepisami prawa handlowego i szeregiem wewnętrznej dokumentacji. Podobnie właściwe zarządzanie ryzykiem, które pozwoli zminimalizować prawdopodobieństwo wystąpienia incydentów.

Czas start, czyli jak powinien wyglądać harmonogram działań

Prace związane z dostosowaniem przedsiębiorstwa obejmują cztery główne etapy – ustalenie swojego statusu, weryfikację funkcjonującego już w firmie systemu cyberbezpieczeństwa, zidentyfikowanie zakresu niezbędnych zmian w tym systemie, a na końcu - wdrożenie nowych lub dostosowanie istniejących rozwiązań. Ustawa o krajowym systemie cyberbezpieczeństwa określa terminy na wykonanie poszczególnych działań w przypadku operatorów usług kluczowych. Pierwsze prace muszą być wykonane już 3 miesiące od daty otrzymania decyzji o uznaniu za operatora. Dotyczy to w szczególności stworzenia struktur odpowiedzialnych za cyberbezpieczeństwo i zidentyfikowania błędów lub braków w zakresie środków bezpieczeństwa. Po 6 miesiącach powinna powstać pełna dokumentacja i procedury w zakresie cyberbezpieczeństwa, a sam system bezpieczeństwa powinien już w pełni działać na nowych zasadach. W przypadku podmiotów publicznych ustawa nie formułuje określonych terminów. Oznacza to, że podmioty publiczne muszą realizować określone działania od dnia wejście w życie ustawy o krajowym systemie cyberbezpieczeństwa, czyli 28 sierpnia 2018 r. Dlatego dla tych podmiotów wdrożenie wymogów dotyczących cyberbezpieczeństwa jest już mocno palącym tematem.

Za błędy lub braki odpowie zarząd

Standardowo za prawidłowe prowadzenie działalności przez przedsiębiorstwo energetyczne odpowiadają osoby, które nim zarządzają. Nie inaczej jest również w przypadku przepisów o cyberbezpieczeństwie, które przewidują dwóch adresatów kary administracyjnej. Za nieprzestrzeganie przepisów zapłaci przede wszystkim przedsiębiorstwo. Kwoty kary dla operatorów usług kluczowych w zależności od rodzaju

naruszenia wahają się od 1.000 do 150.000 zł, przy czym niektóre stawki określono dla pojedynczego naruszenia. W przypadku kilku lub kilkunastu podobnych zdarzeń łatwo stwierdzić, jakich kwot może sięgać kara. Dodatkowo organ właściwy do spraw cyberbezpieczeństwa może za określone nieprawidłowości nałożyć na kierownika operatora usługi kluczowej karę do wysokości 200% miesięcznego wynagrodzenia, wystarczy, ze stwierdzi brak należytej staranności. Tematyka cyberbezpieczeństwa powinna więc trafić na listę spraw szczególnie ważnych dla osób zarządzających.

Autor: Monika Bogdał, radca prawny, Kancelaria Prawna Piszcz i Wspólnicy