Aleksandra Musielak,
Departament Prawa Gospodarczego, Konfederacja Lewiatan

Nowe wymogi z zakresu cyberbezpieczeństwa

- czego może oczekiwać biznes w Polsce (perspektywa prawna)

Polska jest obecnie w punkcie zwrotnym, jeżeli chodzi o kształtowanie nowego cyberładu wewnętrznego oraz zdefiniowanie swojego miejsca na europejskiej i międzynarodowej mapie cyberbezpieczeństwa. Cyberbezpieczeństwo to obszar podlegający obecnie bardzo dynamicznym zmianom, począwszy od nowych organów odpowiedzialnych za politykę cyberbezpieczeństwa, po nowe obowiązki, z którymi przyjdzie się zmierzyć administracji, ale również wielu przedsiębiorstwom działającym na rodzimym rynku. Niniejsza publikacja koncentruje się na zmianach istotnych z perspektywy firm działających na rynku polskim - obecnych i przyszłych uczestników krajowego systemu cyberbezpieczeństwa.

Zmiana ustawy o krajowym systemie cyberbezpieczeństwa

W 2018 r. w Polsce stworzone zostały podstawy Krajowego Systemy Cyberbezpieczeństwa (dalej: „KSC"), którego celem jest podejmowanie sprawnych działań na rzecz wykrywania, zapobiegania i minimalizowania skutków ataków, które naruszają cyberbezpieczeństwo w Polsce. Powstała struktura obejmująca m. in. administrację rządową i samorządową oraz - co istotne - największych przedsiębiorców z kluczowych sektorów gospodarki.

Rząd polski jest obecnie na etapie przemodelowania wspomnianego systemu instytucji tworzących KSC oraz modyfikacji wymogów stawianych administracji oraz biznesowi. Zmiany wynikają z doświadczeń ostatnich dwóch lat funkcjonowania systemu, ale również z potrzeby dostosowania się do wymogów unijnych (konieczność dostosowania się m. in. do unijnego zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G, tzw. „5G Toolbox").

W związku z przygotowaniami do aukcji 5G w Polsce (która jest planowana na 2021 r.), wysiłki administracji koncentrują się wokół właściwego określenia wymogów cyberbezpieczeństwa dla sieci 5G. Komercyjne uruchomienie technologii mobilnej piątej generacji w Polsce jest jedną z ważniejszych i większych krajowych inwestycji infrastrukturalnych, stając się dźwignią rozwoju szeregu kluczowych innowacyjnych produktów i usług w kluczowych sektorach, takich jak: energetyka, transport, bankowość i opieka zdrowotna. Z uwagi na większą zależność od oprogramowania, mniej scentralizowaną architekturę oraz użycie inteligentnej mocy obliczeniowej w architekturze rozproszonej, ten typ sieci wymaga zapewnienia zwiększonego poziomu cyberbezpieczeństwa.

Kluczowe wymagania w tym zakresie zdefiniuje Prezes Urzędu Komunikacji Elektronicznej, któremu w 2020 r. przyznano nowe uprawnienia określania wymogów w zakresie w zakresie bezpieczeństwa i integralności infrastruktury telekomunikacyjnej oraz usług - po zasięgnięciu opinii Kolegium ds. Cyberbezpieczeństwa i z uwzględnieniem rekomendacji i wytycznych Europejskiej Agencji do spraw Bezpieczeństwa Sieci i Informacji (dalej: ENISA).

Po drugie, wysiłki rządu skupione są wokół dostosowania i włączenia podmiotów działających na rynku komunikacji elektronicznej do krajowego systemu cyberbezpieczeństwa. Przedsiębiorcy świadczący usługi komunikacji elektronicznej lub dostarczający sieci telekomunikacyjne zapewnią obsługę incydentu. Przeprowadzą systematyczną ocenę ryzyka wystąpienia sytuacji szczególnego zagrożenia i zobowiązani będą podjąć środki techniczne i organizacyjne, zapewniające poziom bezpieczeństwa adekwatny do poziomu zidentyfikowanego ryzyka.

Planuje się wzmocnienie roli Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa (dalej: ,,Pełnomocnik"), czyli osoby odpowiedzialnej za koordynowanie na poziomie krajowym realizacji zadań dotyczących cyberbezpieczeństwa w Rzeczypospolitej Polskiej. Jego uprawnienia zostaną poszerzone o możliwość wydawania ostrzeżeń - w przypadku uzyskania informacji o zagrożeniu cyberbezpieczeństwa, która uprawdopodobni możliwość wystąpienia incydentu krytycznego oraz poleceń zabezpieczających, w przypadku wystąpienia incydentu krytycznego.

Swoją rolę zmieni Kolegium ds. Cyberbezpieczeństwa (dalej: „Kolegium"). Z ciała opiniodawczo-doradczego stanie się podmiotem z prawem do dokonywania oceny ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów KSC. Kolegium owo ryzyko określi na poziomie wysokie, umiarkowane lub niskie. Ocena wysoka rzutować będzie na niemożność wprowadzania przez daną firmę do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu lub oprogramowania i konieczność wycofania z użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy, nie później niż 5 lat od dnia ogłoszenia komunikatu o ocenie.

Warto zwrócić uwagę na administracyjne kary pieniężne przewidziane za niestosowanie się do obowiązków określonych w ustawie (nakładane na dostawców ocenionych jako kreujących ryzyko umiarkowane oraz wysokie). W przypadku dostawców usług kluczowych nie stosujących się do obowiązków, kara ma wynieść do 3% całkowitego rocznego światowego obrotu firmy z poprzedniego roku obrotowego, podczas gdy dla dostawców z poziomem umiarkowanym wynosi ona odpowiednio do 1% obrotu.

Dyskusje dot. projektu, w szczególności roli Pełnomocnika i Kolegium, wciąż trwają wewnątrz rządu. Nowa wersja projektu, zgodnie z zapowiedziami, ma przyjąć odmienne podejście regulacyjne, z uwzględnieniem procedury opartej na obiektywnych, technologicznych (a nie tylko geopolitycznych) przesłankach oceny dostawców sprzętu i oprogramowania, mając na uwadze skutki dla konkurencyjności rynku, koszty wdrożenia zmian, potrzebę uniknięcia zarzutu dyskryminacji firm działających na rynku krajowym. Projektu w nowej odsłonie można się spodziewać w pierwszym kwartale 2021 r.


fot. freeimages.com

Certyfikacja oraz badania i rozwój

Novum na rynku to zainicjowanie tzw. unijnych certyfikatów cyberbezpieczeństwa. Będą one potwierdzać, że produkty, usługi i procesy ICT są zgodne z określonymi wymogami bezpieczeństwa mającymi na celu zabezpieczenie dostępności, autentyczności, integralności lub poufności przechowywanych, przekazywanych lub przetwarzanych danych, bądź funkcji lub oferowanych usług w trakcie ich całego cyklu życia.

Promotorem pomysłu certyfikacji jest UE, która przyjęła, że system certyfikacji powinien funkcjonować jako dobrowolny. Polska ma czas do czerwca 2021 r. na implementację omawianych wymogów. Dotychczasowe założenia dot. certyfikacji wskazują na to, że system krajowy zostanie oparty na działalności prywatnych jednostek certyfikujących i laboratoriów, a nadzór nad ich działalnością sprawować będzie minister właściwy do spraw informatyzacji oraz Polskie Centrum Akredytacji.

Równolegle UE wspiera wysiłki Państw członkowskich w zakresie wzmacniania inwestycji w badania i rozwój nad cyberbezpieczeństwem. Temu służyć będzie przyszłe Europejskie Centrum Cyberbezpieczeństwa ulokowane w Bukareszcie (decyzja o jego powstaniu zapadła w grudniu 2020 r.). Nowe ciało będzie odpowiadać za zarządzanie miliardowymi funduszami przeznaczonymi na badania, zapewnienie wsparcia finansowego i technicznego dla startupów zajmujących się cyberbezpieczeń-

stwem. Przed przedsiębiorcami w Polsce otwierają się zatem możliwości korzystania z nowych, ciekawych form wsparcia rozwoju niezawodnego, bezpiecznego i otwartego ekosystemu cyberbezpieczeństwa.

Dyrektywa NIS2 - dalsze zmiany w cyberprzestrzeni

To nie koniec zmian w obszarze cyberbezpieczeństwa. W grudniu 2020 r. Komisja Europejska opublikowała projekt nowej Strategii Cyberbezpieczeństwa UE oraz dyrektywy NIS 2[1] . Celem wspomnianej dyrektywy jest reforma systemu cyberbezpieczeństwa UE, zmierzająca do objęcia wymogami cyber szerszej grupy przedsiębiorców i wzmocnienie wymogów cyberbezpieczeństwa względem firm.

Prace nad wspomnianą regulacją dopiero się zaczęły i już obecnie można przewidywać, że negocjacje w Brukseli potrwają co najmniej 2 lata.

Zgodnie z założeniami, dotychczasowe wymogi cyberbezpieczeństwa wynikające z dyrektywy NIS (jeżeli chodzi o biznes) ulegną rozszerzeniu o:

- przedsiębiorstwa dostarczające sieci i usługi łączności elektronicznej,
- gospodarkę ściekami i odpadami,
- wytwarzanie niektórych produktów kluczowych (wyroby farmaceutyczne, urządzenia medyczne, elektroniczne, elektryczne, silnikowe),
- przedsiębiorców - producentów jedzenia,
- usługi cyfrowe ujęte szerzej (oprócz dotychczasowych online marketplaces i wyszukiwarek, również usługi chmurowe, centra obliczeniowe, dostawców treści),
- sektor kosmiczny,
- usługi pocztowe i kurierskie.

UE zamierza wyeliminować rozróżnienie między operatorami usług kluczowych, a dostawcami usług cyfrowych. Podmioty będą klasyfikowane w zależności od ich znaczenia i dzielone odpowiednio na kluczowe i ważne (essential i important). Przedsiębiorcy uznani za dostarczający usługi kluczowe (które obejmą m. in. usługi przetwarzania w chmurze), będą zobligowani do wdrożenia adekwatnych środków bezpieczeństwa dla potrzeb niezakłóconego świadczenia usług i podlegać zwiększonemu nadzorowi ze strony administracji. Łagodniej będą potraktowani przedsiębiorcy, którzy uznani zostaną za dostawców ważnych usług. Ich obowiązki obejmą składanie raportów na temat zidentyfikowanych incydentów bezpieczeństwa.

Projekt zaostrza wymogi bezpieczeństwa dla przedsiębiorstw poprzez narzucenie zastosowania przez nie odpowiedniego podejścia do zarządzania ryzykiem bezpieczeństwa sieci i systemów informatycznych (obejmującego wdrożenie środków technicznych i organizacyjnych), wskazując minimalny wykaz podstawowych elementów bezpieczeństwa, które muszą być przez przedsiębiorców stosowane.

Środki te obejmują co najmniej następujące elementy:

- analizę ryzyka i polityki bezpieczeństwa systemu informatycznego,
- obsługę incydentów (zapobieganie, wykrywanie i reagowanie na incydenty),
- ciągłość działania i zarządzanie kryzysowe,
- bezpieczeństwa łańcucha dostaw, w tym aspektów związanych z bezpieczeństwem dotyczącym relacji między każdym podmiotem, a jego dostawcami lub usługodawcami, takimi jak: dostawcy usług przechowywania i przetwarzania danych lub zarządzanych usług bezpieczeństwa,
- bezpieczeństwo w zakresie pozyskiwania, rozwoju i utrzymania sieci i systemów informatycznych, w tym obsługę i ujawnianie podatności,
- polityki i procedury (testowanie i audyt) służące do oceny skuteczności środków zarządzania ryzykiem w zakresie bezpieczeństwa cybernetycznego,
- stosowania kryptografii i szyfrowania.

Projekt odnosi się do kwestii bezpieczeństwa łańcuchów dostaw i stosunków z dostawcami poprzez nałożenie na poszczególne przedsiębiorstwa wymogu zajęcia się zagrożeniami bezpieczeństwa cybernetycznego w łańcuchach dostaw i stosunkach z dostawcami. Na szczeblu europejskim projekt wzmacnia bezpieczeństwo cybernetyczne łańcucha dostaw w przypadku kluczowych technologii informacyjno-komunikacyjnych.

Pojawią się nowe ramy ujawniania podatności w odniesieniu do nowo odkrytych podatności w całej UE oraz utworzony zostanie unijny rejestr podatności prowadzony przez ENISĘ.

UE zamierza również wprowadzić bardziej rygorystyczne środki nadzoru i egzekwowania przepisów, obejmujący sankcje administracyjne, w tym grzywny za naruszenie przepisów. Projekt pozostawia państwom członkowskim UE ustalenie ich wysokości.

Wnioski

Unia Europejska, jak i organy krajowe stawiają sobie ambitne cele związane z szybkim, a zarazem dalekosiężnym wdrożeniem rozwiązań służących poprawie cyberbezpieczeństwa. Za tymi zmianami muszą podążać przedsiębiorcy, będący kluczowym ogniwem KSC, poddani konieczności wdrożenia szeregu nowych, często kosztownych wymagań. Planowane w najbliższym czasie zmiany rzutować będą na funkcjonowanie coraz szerszej grupy branż działających w Polsce. By być w pełni przygotowane, firmy powinny z uwagą, oprócz nowinek technologicznych, śledzić nowe trendy, w tym podstawowe regulacje i dokumenty strategiczne kształtujące politykę cyberbezpieczeństwa w Polsce. □

[1] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148).