TELKOIN

Wdrożenie przepisów ustawy o krajowym **systemie cyberbezpieczeństwa**

Technologiczne i prawne wyzwania

Przygotowane przy wsparciu merytorycznym
Kancelarii Prawnej Media

MEDIA
KANCELARIA PRAWNA

SPIS TREŚCI

Cyberbezpieczeństwo w praktyce: jak będzie wyglądać wdrażanie KSC/NIS2?

Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa zbliża się nieuchronnie, a wraz z nią nowe standardy związane z zapewnianiem bezpieczeństwa sieci. Warto już teraz zapoznać się z nowymi wymogami i rozpocząć przygotowania do wdrożenia zmian w organizacjach. W tym artykule zarysujemy naszą propozycję, jak należy zabrać się za ten proces i wyjaśnimy, na czym on ma polegać.

Czym są NIS2 oraz KSC i jakie zmiany za sobą niosą?

NIS2 to unijna dyrektywa, która wprowadza środki podnoszące poziom cyberbezpieczeństwa w UE. Jako że dyrektywa ze swojej natury wymaga implementacji, będzie ona obowiązywać w naszym kraju dopiero po wprowadzeniu jej postanowień do polskich przepisów. Temu właśnie służyć ma nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa, czyli KSC. Prace nad nowelizacją jeszcze trwają, ale przewiduje się, że jej uchwalenie może nastąpić około połowy bieżącego roku.

Dyrektywie NIS2 przyświeca założenie, że odpowiedni poziom cyberbezpieczeństwa możemy osiągnąć jedynie przez wszechstronne środki, co oczywiście oznacza nowe wyzwania dla przedsiębiorców. Bezpieczeństwo ma bowiem wynikać nie tylko z wprowadzenia środków technicznych, ale przede wszystkim z uporządkowania zarządzania całą organizacją. Niezbędne będzie przyjęcie odpowiednich procedur bezpieczeństwa, które powinny być realizowane przez wyznaczone i odpowiednio przygotowane do tego osoby. Sposób realizacji tych procedur i obowiązków będzie podlegać drobiazgowej kontroli, więc nie można podejść do tego lekceważąco.

Jak wyżej wspomniano, realizacja wymogów NIS2/ KSC będzie wymagać zmian w sposobie funkcjonowania całej organizacji. We wdrożenie środków cyberbezpieczeństwa konieczne będzie zatem pełne zaangażowanie kierownictwa. Kadra kierownicza będzie, ponadto, ponosić osobistą odpowiedzialność za efekty wdrożenia. Zgodnie z przepisami kary finansowe za naruszenia KSC będą mogły zostać nałożone nie tylko na organizację, ale również właśnie na kierownika. Nie da się tej odpowiedzialności przenieść na podwładnych.

Od czego zacząć wdrożenie KSC? Czy wystarczą normy ISO?

Analizując kwestię wdrożenia KSC warto mieć świadomość, że nie jest ono równoznaczne z wdrożeniem odpowiednich norm ISO dotyczących cyberbezpieczeństwa. Normy te stanowią ogólne wytyczne i nie są wprost związane z wymogami określonymi w NIS2 i KSC. Te zaś są normami prawnymi, obwarowanymi konkretnymi (i dotkliwymi) sankcjami. Wdrożenie norm ISO oczywiście można uznać za krok w dobrym kierunku, ale nie za gwarancję spełnienia wymogów KSC. Konieczne jest bowiem zmodyfikowanie struktury organizacji w sposób, który nie tylko spełni wymogi KSC, ale jednocześnie zapewni zgodność i spójność z innymi obowiązkowymi regulacjami, jak np. Prawo komunikacji elektronicznej, ustawa o zwalczaniu nadużyć w komunikacji elektronicznej, RODO, czy inne akty prawne. Zalecamy zatem podejście uwzględniające specyfikę działalności przedsiębiorców telekomunikacyjnych.

Wdrożenie KSC powinno zacząć się od przeprowadzenia analizy ryzyka. Ten proces powinien zostać wykonany świadomie i z uwzględnieniem skrupulatnego zbadania stanu wyjściowego całej organizacji. Należy rozpoznać m. in. jakimi zasobami dysponuje organizacja, jakie role i odpowiedzialności przypisane są konkretnym osobom, jak również kim są kontrahenci, klienci, czy też dostawcy sprzętu i oprogramowania. Trzeba również ustalić obowiązujące procedury dotyczące cyberbezpieczeństwa - nawet jeżeli dotychczas nie zostały spisane. Po takim badaniu organizacji należy wykonać analizę SWOT, która pozwoli uporządkować ryzyka zewnętrzne i wewnętrzne dla organizacji, aby w efekcie wykonać pełną analizę ryzyka.

Dopiero mając pełny obraz organizacji i zagrażających jej niebezpieczeństw można zdecydować o tym, jak mają być chronione systemy informacyjne oraz które z nich powinny podlegać monitorowaniu w trybie ciągłym. Tu znowu uwydatnia się rola kierownictwa, które powinno ustalić priorytety firmy oraz podjąć decyzję co do sposobu reagowania na cyberzagrożenia i incydenty. Należy również dobrać odpowiednie środki techniczne, takie jak systemy monitorowania sieci. Zawsze należy podejść do tego indywidualnie, aby dobrać takie rozwiązania, których organizacja rzeczywiście potrzebuje i będzie faktycznie z nich korzystać. Nie do przecenienia jest tutaj rola doświadczonych wdrażających, którzy będą wiedzieli, jakie elementy należy zmienić, a jakie mogą pozostać „po staremu". Dostosowanie zakresu zmian do indywidualnych potrzeb z pewnością ułatwi też racjonalizację kosztów.

Komu przedsiębiorcy telekomunikacyjni powinni powierzyć wdrożenie KSC?

W przekonaniu Kancelarii Prawnej Media, najbardziej optymalne i bezpieczne wdrożenie KSC wymaga zaangażowania zespołu interdyscyplinarnego. Potrzebni są do tego zarówno prawnicy, audytorzy ISO, jak również kompetentni informatycy. Przede wszystkim jednak nie da się przeprowadzić tego procesu bez zaangażowania kierownictwa, o czym mowa była wcześniej.

Dzięki skutecznej współpracy specjalistów z kierownictwem wdrożenie może zakończyć się opracowaniem procedur skutecznych i stale realizowanych w organizacji. Nic nie wniesie utworzenie procedur, jeżeli następnie zostaną one schowane do szuflady. Realizacja postanowień KSC będzie w przyszłości podlegać kontrolom, które będą m.in. ustalać istnienie dowodów na przestrzeganie procedur. Warto przypomnieć, że nowelizacja ustawy KSC będzie zawierać katalog surowych kar finansowych, grożących organizacjom i ich kierownikom za nieprzestrzeganie przepisów. Nie zapominajmy też, że NIS2 i KSC to nie tylko obowiązki, ale też szansa na zabezpieczenia przed realnymi zagrożeniami, których liczba rośnie w zastraszającym tempie. Stąd tak ważne jest właściwe dobranie rozwiązań dla danej organizacji.

Dominik Tokarski
radca prawny

W niniejszym dodatku zawarty został obszerny wywiad, którego dla portalu TELKO.in udzieliła Kinga Pawłowska-Nojszewska z Kancelarii Prawnej Media - radca prawny z rozległym doświadczeniem w doradztwie z zakresu cyberbezpieczeństwa, w tym na rzecz klientów objętych obowiązującymi od 2018 roku przepisami ustawy KSC. W ramach wywiadu Czytelnicy otrzymają dalsze, praktyczne informacje na temat wdrażania KSC/NIS2, a także wskazówki na temat tego, jak można się przygotować na ten proces.

Ponadto niniejszy dodatek zawiera artykuł „Praktyczne przygotowanie do zgodności z NIS2/KSC", przygotowany przez Tomasza Procia z Kancelarii Prawnej Media – radcę prawnego z bogatym doświadczeniem w przygotowywaniu organizacji do stosowania polskich i unijnych regulacji. Czytelnicy artykułu otrzymają również możliwość darmowego pobrania wzoru polityki bezpieczeństwa i ciągłości łańcucha dostaw produktów ICT, usług ICT i procesów ICT.

Dodatkowo już **15 maja 2025 r.** Kancelaria Prawna Media zaprasza na webinar pt. ***„Przedsiębiorca telekomunikacyjny, hostingodawca i szerzej: sektor infrastruktury cyfrowej. Od czego zacząć wdrażanie NIS2/KSC?."***

Wydarzenie skierowane jest do przedstawicieli firm i instytucji poszukujących praktycznych wskazówek, jak bez zbędnej teorii, krok po kroku i skutecznie wdrożyć NIS2/KSC.

ZAREJESTRUJ SIĘ TUTAJ

Ustawa o KSC to nie cyberzagadka

Przy wdrażaniu przepisów znowelizowanej ustawy o KSC najbardziej złożonymi obowiązkami wydają się te dotyczące zapewnienia bezpieczeństwa łańcucha dostaw. Jest to zadanie złożone i wieloaspektowe, a wymagania stawiane przez podmioty kluczowe i ważne przełożą się także na ich podwykonawców – mówi ***Marcin Wysocki****, zastępca dyrektora Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji. Jest on przekonany, że gdy nowe wymogi zaczną być wdrażane, będziemy jako kraj lepiej przygotowani na aktualne i ewoluujące wyzwania w obszarze cyberbezpieczeństwa.*

Marcin Wysocki
zastępca dyrektora
Departamentu Cyberbezpieczeństwa
w Ministerstwie Cyfryzacji

TELKO. in: Na jakim etapie jest proces procedowania nowelizowanej ustawy o Krajowym Systemie Bezpieczeństwa (KSC) i czy w resorcie jest jakiś horyzont czasowy, kiedy przepisy dyrektywy NIS 2, które ma implementować ta ustawa, zaczną obowiązywać w Polsce?

MARCIN WYSOCKI, zastępca dyrektora Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji, Projekt nowelizacji ustawy o krajowym systemie bezpieczeństwa (ustawy o KSC) jest na etapie prac rządowych i zostanie niebawem przekazany do rozpatrzenia przez Stały Komitet Rady Ministrów. Staramy się, aby ustawa została uchwalona do końca I połowy 2025 r. i weszła w życie w bieżącym roku, natomiast w przypadku wielu podstawowych obowiązków dla administracji i przedsiębiorców objętych regulacją – w szczególności dotyczących wdrożenia systemu zarządzania bezpieczeństwem informacji – przewidziany jest aktualnie 6-miesięczny termin *vacatio legis*.

Jako kraj mamy już spore opóźnienie we wdrażaniu NIS 2, co powinno nastąpić w połowie października ub. roku. Czy grożą za to nam jako państwu kary, jak to było w przypadku PKE?

Polska jest jednym z kilkunastu krajów, które nie dokonały jeszcze transpozycji tzw. dyrektywy NIS 2. Biorąc pod uwagę stan transpozycji w innych krajach UE, obecnego opóźnienia nie określiłbym jako „spore". Natomiast zostało wszczęte postępowanie w związku z naruszeniem zobowiązań państwa członkowskiego i groźba kar jest realna. W związku z tym pojawiające się w przestrzeni publicznej postulaty „zamrożenia" prac nad ustawą lub ich restartu nie są „bezkosztowe" – ewentualne kary za brak transpozycji w terminie finansują podatnicy, czyli my wszyscy.

A jak w samym ministerstwie przebiegają prace nad przygotowywaniem się do wdrożenia NIS 2 w Polsce? Jaką rolę będzie pełnił resort w systemie cyberbezpieczeństwa państwa, gdy wejdą w życie przepisy?

Nowe przepisy oznaczają przede wszystkim wzmocnienie kompetencji zarówno Ministra Cyfryzacji, jak i Pełnomocnika Rządu ds. Cyberbezpieczeństwa.

Minister Cyfryzacji będzie tzw. organem właściwym do spraw cyberbezpieczeństwa m.in. dla administracji publicznej, w tym jednostek samorządu terytorialnego. Będzie miał z jednej strony kompetencje do wspierania – razem z CSIRTami – podmiotów regulowanych, z drugiej zaś strony – do prowadzenia kontroli i ewentualnych postępowań o nałożenie kary w przypadku nieprzestrzegania przepisów ustawy. Ustawa pozwoli również skutecznie działać w związku z wystąpieniem incydentu krytycznego (w postaci wydania polecenia zabezpieczającego). Umożliwi także zadbanie o cyberbezpieczeństwo na poziomie strategicznym, ponieważ to Minister Cyfryzacji będzie gospodarzem postępowania o uznanie danego dostawcy za dostawcę wysokiego ryzyka.

Nowe przepisy wzmocnią również pozycję Pełnomocnika Rządu ds. Cyberbezpieczeństwa – od współpracy w ramach połączonego Centrum Operacji w Cyberprzestrzeni czy Zespołu Incydentów Krytycznych po wydawanie przez Pełnomocnika rekomendacji określających środki techniczne i organizacyjne stosowane w celu zwiększenia bezpieczeństwa systemów informacyjnych wszystkich podmiotów krajowego systemu cyberbezpieczeństwa.

W Departamencie Cyberbezpieczeństwa Ministerstwa Cyfryzacji zbudowaliśmy kompetentny i zgrany zespół, który jest gotowy do podjęcia nowych zadań i realizacji kolejnych ambitnych celów.

Na ile firmy w Polsce są przygotowane do wdrożenia NIS 2? Niektórzy szacują, że nowe przepisy obejmą około 38 tys. firm. Czy to realne dane?

Nowe przepisy obejmą około 38 tys. podmiotów, z czego 28 tys. to podmioty kluczowe i ważne z sektora administracji publicznej. Szczegółowe wyliczenia Ministerstwa Cyfryzacji w podziale na konkretne podmioty i rodzaje podmiotów są zawarte w ocenie skutków regulacji projektowanej ustawy (w stosownych przypadkach odnosimy się do kodów PKD).

Przedsiębiorstwa w Polsce z pewnością są różnie przygotowane do wdrożenia nowych przepisów, ale i oczekiwania regulacyjne wobec nich są zróżnicowane. Dyrektywa NIS 2 obejmuje wiele sektorów, w których występują średni

i duzi przedsiębiorcy, a także – jak w sektorze infrastruktury cyfrowej – nawet mikroprzedsiębiorcy i mali przedsiębiorcy. Zgodnie z dyrektywą przy nakładaniu obowiązków należy uwzględnić sytuację podmiotów, którymi mogą być wielcy operatorzy sieci mobilnych, lokalni dostawcy dostępu do Internetu czy lokalni przedsiębiorcy wodociągowi. Każda z tych usług ma swoją specyfikę, dlatego – wdrażając środki techniczne i organizacyjne – podmiot powinien wybrać takie, które będą dopasowane do jego wielkości, charakteru świadczonych usług, możliwości finansowych, aktualnej wiedzy technicznej czy cyberzagrożeń. Jednocześnie środki te powinny być ze sobą zharmonizowane (proporcjonalne) – na przykład rozbudowany dział cyberbezpieczeństwa, z politykami bezpieczeństwa i odpowiednim SIEM (Security Information and Event Management - system do zarządzania informacjami i zdarzeniami dotyczącymi bezpieczeństwa w organizacji) nie będzie efektywny, jeżeli zaniedbane zostanie szkolenie personelu z higieny cyfrowej. Chcemy uniknąć nakładania nadmiernych obowiązków na podmioty dzięki uelastycznieniu przepisów i zapewnieniu zindywidualizowanego podejścia.

Czy nowelizacja KSC rzeczywiście oznacza rewolucję dla wielu firm w zakresie cyberbezpieczeństwa, czy jest raczej największą cyberzagadką 2025 r., jak to nazwała jedna z dużych firm prawniczych w tytule zaproszenia na seminarium na ten temat?

Jesteśmy kilkanaście lat po wejściu w życie rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności oraz prawie 7 lat po wdrożeniu RODO i ustanowieniu krajowego systemu cyberbezpieczeństwa. Świadomość Polaków w tym zakresie rośnie, podobnie jest w przypadku administracji i przedsiębiorców.

W tym kontekście cyberincydent wiąże się nie tylko z ewentualną karą administracyjną nakładaną przez Prezesa Urzędu Ochrony Danych Osobowych w związku z wyciekiem danych osobowych. To również straty wizerunkowe, utrata zaufania klientów czy możliwa strata np. informacji objętych tajemnicą przedsiębiorstwa.
Potrzebna jest oczywiście szeroka i skuteczna komunikacja planowanych zmian, natomiast w projektowanej nowelizacji ustawy o KSC są narzędzia do tego, żeby mobilizować podmioty istotne z perspektywy funkcjonowania państwa do zadbania o cyberbezpieczeństwo. Uświadamianie im, jak ważne jest cyberbezpieczeństwo, wymaga pracy wielu instytucji publicznych i prywatnych. Działania te są już realizowane.

Które sektory w Polsce objęte przepisami NIS 2 są najlepiej do tego przygotowane, a gdzie to wygląda najgorzej?

Z pewnością najlepiej przygotowane są sektory, w których już dzisiaj zostali wyznaczeni operatorzy usług kluczowych. Z kolei największe wyzwania czekają „nowe sektory" (nowe z perspektywy włączenia ich do krajowego systemu cyberbezpieczeństwa, tzn. te, których obecna ustawa nie dotyczy), takie jak produkcja ogólna, produkcja i dystrybucja chemikaliów, produkcja i dystrybucja żywności, zarządzanie ICT, ścieki itd. W tym ostatnim przypadku będzie możliwość uzyskania grantu w ramach programu „Cyberbezpieczne wodociągi", którego celem jest zwiększenie odporności na cyberzagrożenia przedsiębiorstw wodociągowo-kanalizacyjnych.

Które z nowych wymogów mogą być dla przedsiębiorstw najtrudniejsze do spełnienia, a które najkosztowniejsze?

Najbardziej złożonymi obowiązkami wydają się te dotyczące zapewnienia bezpieczeństwa łańcucha dostaw. Jest to zadanie złożone i wieloaspektowe, a wymagania stawiane przez podmioty kluczowe i ważne przełożą się także na ich podwykonawców. Niezbędną są analizy i stawianie wysokich wymogów z zakresu cyberbezpieczeństwa także wobec kontraktorów, którymi mogą być tzw. giganci cyfrowi lub monopoliści na danym specyficznym, ograniczonym rynku.

Chyba jednymi z najczęściej kwestionowanych przepisów nowelizacji ustawy o KSC jest kwestia dostawców wysokiego ryzyka. Padają m.in. zarzuty, że pisane były one były pod dyktando Amerykanów, którzy prowadzą wojnę gospodarczo-technologiczną z Chinami. Ministerstwo jednak mocno obstaje przy tych zapisach. Dlaczego?

Przepisy dotyczące dostawców wysokiego ryzyka są wyrazem dążenia Polski i całej Unii Europejskiej do zapewnienia cyberbezpieczeństwa w wymiarze strategicznym i nie były pisane pod niczyje dyktando. Mają zapewnić instytucje prawne o charakterze ochronnym, których nie można osiągnąć innymi, nie tak daleko idącymi działaniami.

Polska w dalszym ciągu nie wdrożyła unijnego zestawu środków dla cyberbezpieczeństwa sieci 5G – tzw. Toolbox 5G. Jesteśmy jednym z ostatnich państw Unii Europejskiej bez horyzontalnej regulacji procedury uznawania za dostawcę wysokiego ryzyka. Ustanowienie tej procedury to kwestia realizacji podstawowych interesów Polski w obszarze bezpieczeństwa.

Lobbowanie o jej usunięcie (oparte na nieprawdziwej informacji, że rzekomo nie jesteśmy zobowiązani do wdrożenia Toolbox 5G) jest – jak wskazuje wicepremier i minister cyfryzacji Krzysztof Gawkowski – de facto cyfrową zdradą stanu.

Firma EY w swej niedawnej krytycznej analizie, w której stawia tezę, że wiele z proponowanych w nowelizowanej ustawie o KSC w Polsce to nadregulacja, wskazuje m.in., że Polska jako jedyny kraj w Europie planuje wdrożenie 5G Tolboox w 18 sektorach gospodarki. Tymczasem żadne z państw UE nie wprowadza zaleceń 5G Toolbox w infrastrukturze innej niż telekomunikacyjna. Czy to rzeczywiście nadgorliwość?

Zgodnie z NIS 2 wszystkie podmioty kluczowe i ważne mają obowiązek wdrożyć środki zapewniające bezpieczeństwo łańcuchów dostaw. Obowiązek ten nie dotyczy więc tylko sektora telekomunikacyjnego. Ponadto podmioty kluczowe i podmioty ważne mają uwzględnić wyniki skoordynowanego szacowania ryzyka przeprowadzonego wobec konkretnego dostawcy przez Grupę Współpracy NIS. Pierwowzorem tego postępowania była unijna ocena cyberbezpieczeństwa sieci 5G, na podstawie której powstał Toolbox 5G. Aspekt bezpieczeństwa łańcuchów dostaw jest zatem uwzględniony w dyrektywie NIS 2.

Ryzykowni dostawcy mogą występować nie tylko w sektorze telekomunikacyjnym, ale też w innych sektorach. W jednym ze swoich raportów Grupa Współpracy NIS wskazała, że czynnikiem sprzyjającym atakom w łańcuchu dostaw w sektorze energetycznym mogą być zależności przedsiębiorstw energetycznych od dostawców sprzętu lub oprogramowania, którzy mogą być uznawani za stwarzających wysokie ryzyko. Dlatego cyberzagrożenia w obszarze łańcuchów dostaw należy ujmować holistycznie i uwzględnić zagrożenia potencjalnie występujące nie tylko w jednym z sektorów, ale również w pozostałych.

Stąd postępowanie w sprawie uznania dostawcy za dostawcę wysokiego ryzyka może dotyczyć dostawcy sprzętu lub oprogramowania dla różnych sektorów. W mojej ocenie w przyszłości będzie tak, jak z naszą krajową definicją „incydentu", która jest szersza niż

wynikająca z pierwszej dyrektywy NIS. Lata doświadczeń i rozwiązania zawarte w dyrektywie NIS 2 potwierdzają, że polskie podejście zaproponowane lata temu było adekwatne i słuszne.

Z drugiej strony, gdy Komisja Europejska rekomenduje zakaz używania sprzętu Huawei, a w Brukseli trwa postępowania dotyczące korumpowania przez chińską firmę europarlamentarzystów, resort cyfryzacji wydał oświadczenie, że nie planuje wprowadzenia zakazu ani ograniczenia używania sprzętu Huawei w polskich sieciach telekomunikacyjnych, w tym 5G. To chaos czy może oświadczenie pisane tym razem pod dyktando chińskich lobbystów?

Stanowisko Ministra Cyfryzacji w tym zakresie jest niezmienne od lat – musimy wprowadzić odpowiednią procedurę. Ze względu na to, że jest to najdalej idący środek prawny, niezbędne jest wprowadzenie odpowiednich gwarancji zapewniających rzetelność procesu, uwzględnienie różnych ważnych aspektów, analiz technicznych, prawnych, a także skutków ewentualnych decyzji. Stawka jest ogromna – są nią podstawowe interesy Polski w zakresie bezpieczeństwa, a skutki indywidualnych decyzji mają swoje konsekwencje m.in. w sferze swobody prowadzenia działalności gospodarczej. Zapowiadanie ewentualnych przyszłych rozstrzygnięć bez pełnego obrazu sytuacji – a taki pozwoli ustalić transparentna i złożona procedura uznania dostawcy za dostawcę wysokiego ryzyka – nie jest w mojej ocenie właściwe.

Apel Komisji mógłby zostać uwzględniony przy analizie spełnienia przesłanek do wszczęcia postępowania dotyczącego uznania za dostawcę wysokiego ryzyka, ale tej procedury jeszcze nie ma. Tutaj dochodzimy do kwestii lobbingu – działań na rzecz przerwania bądź zahamowania prac nad projektem ustawy o krajowym systemie cyberbezpieczeństwa, rozpowszechniania mitów czy półprawd o kwestiach rzekomo stanowiących nadregulację (a w rzeczywistości wynikających wprost z dyrektywy NIS 2) i tym podobnym zabiegów.

Dyrektywa NIS 2 i nowelizacja KSC podniosą poprzeczkę w zakresie wymogów dotyczących ochrony infrastruktury IT. Firmy będą musiały wdrożyć odpowiednie i proporcjonalne środki techniczne oraz organizacyjne, aby skutecznie zarządzać ryzykiem dla swoich systemów IT. Na to trzeba będzie wydać konkretne pieniądze. Czy resort ma jakieś wyliczenia, ile to może kosztować?

Jak już wspomniałem, przedsiębiorstwa są różnie przygotowane na nowe przepisy, ale i oczekiwania regulacyjne wobec nich są odmienne. Wdrażając środki techniczne i organizacyjne, dany podmiot powinien wybrać takie, które będą odpowiednie do jego wielkości, charakteru świadczonych usług, możliwości finansowych, aktualnej wiedzy technicznej czy cyberzagrożeń.

Koszty takich wdrożeń są niestety bardzo trudne do rzetelnego oszacowania. Wyliczenia są związane ze znacznymi uproszczeniami i oparte o wiele niewiadomych. Ocena skutków regulacji do dyrektywy NIS 2 z 2020 roku wskazuje, że podmioty objęte pierwszą dyrektywą NIS jednorazowo miały zwiększyć swoje wydatki na bezpieczeństwo ICT o 22 proc. Dla nowych podmiotów miał być to jednorazowy koszt 25 proc. wydatków na ICT.

Niektórzy szacują, że średni koszt wdrożenia nowych przepisów w przypadku podmiotów prywatnych wyniesie od kilkudziesięciu do kilkuset tysięcy złotych. Czy można ufać tym wyliczeniom?

Proszę zapytać autorów takich szacunków o szczegóły ich wyliczeń. Kiedy zadawałem takie pytania, dostawałem informacje, że w szacunkach brane są pod uwagę np. koszty wymiany ogółu sprzętu ICT od dostawców spoza NATO. Jeżeli tak jest, to nie są to dane wiarygodne.

Istotną częścią dyrektywy NIS 2 w nowelizowanej ustawie KSC jest mechanizm samoidentyfikacji. To na przedsiębiorstwach spoczywać będzie obowiązek oceny, czy ich działalność wpisuje się w ramy regulacji. Jeśli firma uzna, że spełnia kryteria, musi zgłosić się do rejestru prowadzonego przez Ministerstwo Cyfryzacji. Jak będziecie weryfikować czy firmy dokonały właściwie tej samooceny?

Mechanizm samorejestracji wynika z dyrektywy NIS 2. Podmioty regulowane posiadają odpowiednią wiedzę – w szczególności w zakresie swojego obrotu oraz liczby zatrudnianych pracowników – do odpowiedniej klasyfikacji w oparciu o transparentne, znane przesłanki wynikające z dyrektywy NIS 2 i przyszłych przepisów nowelizowanej ustawy o KSC. Kontrola Ministra Cyfryzacji będzie miała charakter następczy, a we wpisie zostaną uwzględnione dane przekazywane przez przedsiębiorców do ZUS w zakresie liczby ubezpieczonych pracowników, jak również dane zawarte w sprawozdaniach finansowych obejmujących roczny obrót. Istotne będą także dane z rejestru REGON, dlatego podjęliśmy się dopasowania kodów PKD do działalności, których dotyczy dyrektywa NIS 2.

Czy po wejściu w życie przepisów o KSC ministerstwo będzie surowo karać tych, którzy będą je naruszać? Kary do niskich chyba nie należą?

Zgodnie z dyrektywą NIS 2 kary muszą być skuteczne, proporcjonalne i odstraszające. Kary spełniają wiele funkcji i są nakładane w sformalizowanym, indywidualnym akcie stosowania prawa – decyzji administracyjnej. W przypadku wyższego progu zakresu naruszenia naprawdę wiele okoliczności uwzględnianych przy miarkowaniu kary musiałaby obciążać stronę takiego postępowania, czyli podmiot dokonujący naruszenia. Punktem odniesienia może być analiza stosowania przepisów przez Prezesa Urzędu Ochrony Danych Osobowych i Prezesa Urzędu Komunikacji Elektronicznej. Tam również przepisy sektorowe przewidują potencjalnie bardzo wysokie kary maksymalne za naruszenia przepisów.

Czy rzeczywiście będziecie co roku kontrolować 10 proc. podmiotów podlegających przepisom ustawy i kto to będzie robił – pracownicy resortu czy wynajęte firmy?

Taka wielkość wydaje się adekwatna. Wyliczenia w ocenie skutków regulacji zakładają odpowiednie zatrudnienie po stronie organów właściwych do spraw cyberbezpieczeństwa, aby te kompetencje realizować. Wielkość próbki podmiotów objętych kontrolą, uwzględniając ich liczbę, według mnie powinna wynosić od kilku do kilkunastu procent rocznie. Nie możemy dopuścić do sytuacji, w której nie będzie odpowiednich środków do przeprowadzenia kontroli i weryfikacji, czy dany podmiot wypełnia obowiązki. Podobnie jak w prawie karnym – występowanie zachowań penalizowanych ogranicza w większym stopniu nieuchronność kary niż jej potencjalna wysokość. Z drugiej strony, na pewno są inne działania, w których kompetencje podmiotów administracji publicznej mogą być bardziej efektywnie wykorzystywane, aby poprawić poziom bezpieczeństwa w Polsce, niż bezrefleksyjne dążenie do kontrolowania jak największej liczby podmiotów w jak najkrótszym czasie.

Ile czasu może minąć, kiedy zaczną być odczuwalne pierwsze efekty odnośnie poprawy cyberbezpieczeństwa w kraju po wejściu w życie przepisów znowelizowanej ustawy o KSC? Czy można być w ogóle pewnym, że poprawa w tym zakresie będzie widoczna.

Czego się spodziewacie jako Ministerstwo Cyfryzacji?

Pierwsze efekty wdrożenia dyrektywy NIS 2 już są widoczne, bo wiele podmiotów ma świadomość, że są „podmiotami NIS" lub „podmiotami KSC 2.0". Spodziewamy się osiągnięcia celów określonych w dyrektywie – zwiększenia bezpieczeństwa w Polsce i w całej Unii Europejskiej. Analizując odpowiednie mierniki, trzeba wziąć pod uwagę szereg okoliczności, bo np. liczba zgłoszonych incydentów może wynikać ze zwiększonej świadomości podmiotów i niekoniecznie musi to oznaczać, że zdolność do zapewnienia cyberbezpieczeństwa w krajowym systemie cyberbezpieczeństwa spadła. Na pewno dzięki nowelizacji ustawy o KSC będziemy jako kraj lepiej przygotowani na aktualne i ewoluujące wyzwania w obszarze cyberbezpieczeństwa.

Dziękujemy za rozmowę.
Rozmawiał Marek Jaślan

Ile wdrożenie nowych przepisów o KSC może kosztować polskich przedsiębiorców?

Od kilkudziesięciu tysięcy złotych dla mniejszych firm do milionów złotych dla większych podmiotów – to koszty, które będą musiały ponieść w Polsce firmy objęte przepisami nowelizowanej ustawy o KSC. Firma EY podkreśla, że to wyliczenia dokonane na rzetelnych podstawach.

Firma EY w swej ubiegłorocznej publikacji „Nowe obowiązki w cyberbezpieczeństwie – ryzyko nadregulacji" stwierdza, że bezpośrednie koszty zmian związanych z nowelizacją KSC będą zróżnicowane w zależności od wielkości oraz specyfiki działalności przedsiębiorstwa, ale na pewno niemałe.

> *– Podstawowym wydatkiem, z którym będą musieli się liczyć przedsiębiorcy, będzie zakup lub aktualizacja systemów IT (w tym zaawansowanych rozwiązań zabezpieczających). Koszty te mogą się wahać od kilkudziesięciu tysięcy złotych dla małych firm, po kwoty liczone w milionach dla dużych korporacji, przetwarzających znaczący wolumen danych. Inwestycje w szkolenia pracowników z zakresu cyberbezpieczeństwa są kolejnym istotnym elementem kosztów nadchodzących zmian. Szkolenia będą niezbędne, aby personel mógł skutecznie zarządzać systemami i reagować na incydenty. Również nowy obowiązek związany z cyklicznym prowadzeniem audytów bezpieczeństwa będzie dodatkowym wydatkiem* – wskazuje EY.

Marcin Wysocki z resortu cyfryzacji w rozmowie, którą publikujemy na *str. 4-6* podważa te szacunki i sugeruje, by zapytać ich autorów o szczegóły ich wyliczeń. Zrobiliśmy to.

EY w odpowiedzi na wątpliwości dotyczące szacunków kosztów wdrożenia nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa, przedstawił nam poniżej zestawienie danych liczbowych i źródłowych, które jego zdaniem – potwierdzają zasadność podanych przedziałów kosztowych – od kilkudziesięciu tysięcy złotych dla mniejszych firm do milionów złotych dla większych podmiotów.

1. Tarlogic – „Between €180,000 and €2 million. This will be the cost of the Cybersecurity Law for companies" (luty 2025)

W hiszpańskiej analizie rządowej, opublikowanej przez firmę Tarlogic, wskazano szacunkowe koszty dostosowania się do nowego prawa transponującego dyrektywę NIS2:

- dla podmiotów ważnych, które dopiero zaczynają wdrożenie: średnio 180 000 euro,
- dla podmiotów ważnych z częściową implementacją: 131 000 euro,
- dla podmiotów kluczowych: od 1,19 mln euro do 2,15 mln euro, w zależności od poziomu zaawansowania,
- dla podmiotów już wcześniej regulowanych: ok. 107 000 euro.

Łączny koszt dla ok. 6 000 przedsiębiorstw w Hiszpanii oszacowano na 2,25 miliarda euro. To kolejny przykład potwierdzający, że skala wydatków dla średnich i dużych firm jest wielomilionowa – zarówno w Polsce, jak i w innych państwach członkowskich Unii Europejskiej.

https://www.tarlogic.com/blog/cost-of-the-cybersecurity-law-companies/?utm_source=chatgpt.com

2. Raport Frontier Economics: „Assessing the Economic Impact of EU Initiatives on Cybersecurity" (2023)

Zgodnie z tym opracowaniem, łączny roczny koszt wdrożenia dyrektywy NIS2 przez przedsiębiorstwa w UE wynosi ok. 31,2 mld euro. Dla „nowych sektorów" objętych regulacją (w tym przemysł, transport, produkcja) oznacza to średnio 0,32 proc. rocznego obrotu firm. Koszty obejmują m.in. sprzęt, licencje, zatrudnienie specjalistów, usługi doradcze i szkolenia. Dla dużych podmiotów, w szczególności działających w infrastrukturze krytycznej lub pokrewnych sektorach, mogą to być inwestycje przekraczające milion euro rocznie. Szacunki te są zgodne z podejściem EY.

https://www.frontier-economics.com/media/izyk5rgz/assessing-the-economic-cost-of-eu-initiatives-on-cybersecurity.pdf

3. White paper AUVESY-MDT: „NIS2 – Stricter Cybersecurity Regulations for Production" (2023)

Dokument koncentruje się na kosztach wdrożenia NIS2 w sektorze produkcyjnym i przemysłowym. Wskazano tam, że przeciętna firma produkcyjna wydaje średnio 40 000 euro na implementację środków zgodnych z dyrektywą. Dla porównania, koszt pojedynczego cyberataku szacowany jest na 100 000 euro, a w produkcji nawet 1,5 mln dol. (dane Sophos). AUVESY-MDT potwierdza również, że nowe regulacje NIS2 obejmują szerszy katalog sektorów niż wcześniejsza wersja dyrektywy, co zwiększa obowiązki i koszty wdrożeniowe po stronie przedsiębiorstw.

https://www.novotek.com/fr/wp-content/uploads/sites/21/whitepaper-nis2-en-2.pdf

---

– Podsumowując, wszystkie trzy źródła jednoznacznie potwierdzają, że wskazywane przez EY przedziały kosztowe są realne i wynikają z zakresu obowiązków prawnych, poziomu dojrzałości infrastruktury IT/OT oraz wymagań organizacyjnych. Utrzymywanie, że koszty te są „niewiarygodne", nie znajduje odzwierciedlenia w dostępnych danych branżowych i rynkowych – stwierdza EY.

Wyliczenia przedstawili:

Justyna Wilczyńska-Baraniak,
partnerka EY, liderka Zespołu Prawa Własności Intelektualnej, Technologii i Danych Osobowych w Kancelarii EY Law,

Szymon Skalski,
associate w Zespole Własności Intelektualnej, Technologii i Ochrony Danych Osobowych w Kancelarii EY Law.

Ile miesięcznie na bezpieczeństwo będą łożyć operatorzy?

W kwietniu tego roku na konferencji KIKE Andrzej Fudala z firmy SayF przedstawiał, jakie miesięcznie koszty mogą ponosić operatorzy telekomunikacyjni z sektora MSP, by spełniać ustawowe obowiązki (w tym NIS2) z zakresu bezpieczeństwa, cyberbezpieczeństwa i obronności. I tak według tych szacunków:

1. Obowiązki na rzecz obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego wynikające z ustawy Prawo Komunikacji Elektronicznej: zapewnienie warunków kontroli informacji przesyłanej w sieci telekomunikacyjnej to koszt co najmniej 12 tys. zł miesięcznie.
2. Cyberbezpieczeństwo – równowartość kosztu zatrudnienia informatyka – administratora systemu informacyjnego to koszt 16 tys. zł miesięcznie.
3. Pozostałe koszty związane z ochroną informacji, np. ochrony danych osobowych, to koszt 2 tys. zł miesięcznie.

W sumie daje to kwotę ok. 32 tys. zł miesięcznie.

Praktyczne przygotowanie do zgodności z NIS2 / nKSC

Ocena Skutków Regulacji projektu nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa (nKSC) wskazuje, że poza podmiotami publicznymi, około 10 tysięcy podmiotów będzie zobowiązanych do przygotowania się do nowych regulacji. Co ciekawe, niemal 4 tysiące z nich to przedsiębiorcy telekomunikacyjni (!). Śmiało można zatem powiedzieć, że branża telekomunikacyjna będzie (ilościowo) jedną z najbardziej dotkniętych regulacją cyberbezpieczeństwa w Polsce. Przed rozpoczęciem prac nad wdrożeniem nKSC warto zwrócić uwagę, że niektóre wymogi ujęte w ustawie będą stosowane tylko do podmiotów ważnych lub podmiotów kluczowych świadczących konkretne kategorie usług.

Wielu przedsiębiorców komunikacji elektronicznej świadczy bowiem również inne usługi, jak np. DNS, przetwarzanie w chmurze, czy rejestracja nazw domen. Przykładem takiego dodatkowego wymogu jest procedura weryfikacji danych przez podmioty świadczące usługi rejestracji nazw domen (por. art. 16a nKSC).

W związku z powyższym, ustalenie katalogu świadczonych usług, które mogą prowadzić do obowiązków na podstawie nKSC, będzie pierwszym etapem przygotowania się do stosowania nowych przepisów. Drugim etapem będzie ustalenie wielkości przedsiębiorstwa, zgodnie z zasadami określonymi w unijnym rozporządzeniu GBER (a nie zgodnie z Prawem przedsiębiorców!), ponieważ w przypadku niektórych usług podleganie pod nKSC będzie warunkowane właśnie wielkością przedsiębiorstwa.

Po ustaleniu, które usługi świadczone przez przedsiębiorcę będą podlegać pod nKSC, można przystąpić do wdrażania jej wymogów. Przygotowanie do stosowania nKSC to wewnętrzne przygotowanie organizacji do wielu przepisów. Wymaga opracowania zasad współpracy z właściwymi organami, ustalenia właściwych polityk i procedur wewnątrz organizacji oraz przypisania pracowników do konkretnych obowiązków.

Jakie to obowiązki? Większość obowiązków została wprost wskazana w projekcie ustawy nowelizującej KSC: jest to m.in. konieczność przygotowania polityki i procedury stosowania kryptografii, czy polityki kontroli dostępu (art. 8 nKSC) lub polityki weryfikacji danych przez podmioty świadczące usługi rejestracji nazw domen (art. 16a nKSC). Inne obowiązki należy wywnioskować z treści przepisów, a ich przykładem jest np. procedura wdrożenia polecenia zabezpieczającego (nie jest wprost wskazana w przepisach, ale podmioty objęte nKSC będą obowiązane wdrożyć określone nakazy ujęte w poleceniu zabezpieczającym, pod rygorem kary (art. 67g i art. 73 nKSC). Jeszcze inne zostały kierunkowo określone w przepisach, lecz w praktyce spełnienie tych obowiązków wymaga przejścia szeregu dodatkowych kroków, tylko pośrednio wynikających z nKSC.

Przykładem tych ostatnich są nowe przepisy dotyczące bezpieczeństwa i łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usługi (art. 8 nKSC).

Projektowana nKSC wyraźnie wskazuje, że system zarządzania bezpieczeństwem informacji w systemie informacyjnym powinien zapewniać wdrożenie środków technicznych i organizacyjnych obejmujących:

- bezpieczeństwo w procesie nabywania, rozwoju, utrzymania i eksploatacji systemu informacyjnego, w tym testowanie systemu informacyjnego,
- bezpieczeństwo i ciągłość łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usługi.

Przepisy nie doprecyzowują, że przedsiębiorcy telekomunikacyjni – jako podmioty kluczowe lub ważne – powinni również posiadać procedurę doboru dostawcy ICT, rejestr dostawców ICT, czy rejestr aktywów ICT. Aby wewnętrzne procedury dotyczące łańcucha dostaw oraz rozwoju, utrzymania i eksploatacji systemu informacyjnego były kompletne, zaś pracownicy wiedzieli, co mają robić, należy uzupełnić procedury o szereg dokumentów pomocniczych – najlepiej wspierając się na dobrych praktykach, które można znaleźć np. w rozporządzeniach wykonawczych dla innych niż stricte telekomunikacja branż lub we właściwych standardach (np. ISO).

W unijnym rozporządzeniu wykonawczym 2024/2690 z dnia 17 października 2024 r., które wyraźnie nie jest dedykowane dla przedsiębiorców telekomunikacyjnych ani przedsiębiorców komunikacji elektronicznej, możemy znaleźć wskazówki, co może znaleźć się w polityce bezpieczeństwa i łańcucha dostaw produktów ICT, usług ICT i procesów ICT oraz bezpieczeństwa w procesie nabywania, rozwoju i utrzymania sieci i systemów informacyjnych. Zgodnie z tym dokumentem zasady bezpieczeństwa łańcucha dostaw obejmują m.in. kryteria wyboru dostawców i usługodawców oraz zasady zawierania z nimi umów, wymogi bezpieczeństwa mające zastosowanie do nabywanych usług ICT lub produktów ICT oraz wymogi dotyczące aktualizacji zabezpieczeń w całym cyklu życia usług ICT lub produktów ICT lub wymiany po zakończeniu okresu wsparcia (por. Załącznik do rozporządzenia wykonawczego 2024/2690, punkt 5.1 i 6.1). Przygotowując dokumentację dotyczącą łańcucha dostaw produktów ICT, usług ICT i procesów ICT należy również pamiętać o dalszych etapach współpracy z dostawcą: zapewnieniu bezpiecznego cyklu rozwoju sieci i systemu informacyjnego, jak również np. regularne testowanie bezpieczeństwa – adekwatne do zidentyfikowanych ryzyk. Właściwe określenie zadań dotyczących bezpieczeństwa i łańcucha dostaw oraz umiejscowienie ich w strukturze organizacyjnej (np. przez przypisanie zadań do konkretnych stanowisk) nie musi znaleźć się w jednym dokumencie. Ważne, aby reguły były jasne i spójne.

Powyżej ujęto jedynie przykłady wymogów stawianych podmiotom regulowanym w nKSC, w tym przedsiębiorcom telekomunikacyjnym. Właściwe przygotowanie organizacji, oraz pracowników, do nowych zadań wymaga spójnych rozwiązań wewnętrznych.

Śmiało można powiedzieć, że nie ma jednego prawidłowego wzoru przygotowania przedsiębiorcy telekomunikacyjnego od nowych przepisów cyberbezpieczeństwa. Warto wzorować się na sprawdzonych praktykach.

Przedstawiamy przykładową *Politykę bezpieczeństwa i ciągłości łańcucha dostaw produktów ICT, usług ICT i procesów ICT*. Zachęcamy do zapoznania się i rozpoczęcia przygotowań do nKSC i NIS2.

LINK : *Polityka bezpieczeństwa i ciągłości łańcucha dostaw produktów ICT, usług ICT i procesów ICT*

Tomasz Proć

Radca prawny z bogatym doświadczeniem w przygotowywaniu organizacji do stosowania polskich i unijnych regulacji.

KONTAKT:
tel. +48 501 448 798
tomasz.proc@kancelaria.media.pl

NIS2 i KSC
– istotne wymogi

Jak jest stan prac nad nowelizacją ustawy o KSC?

Projekt nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa wdrażający na grunt polski NIS2 czeka na przyjęcie przez Radę Ministrów, a następnie na głosowanie w parlamencie. Ministerstwo Cyfryzacji liczy, że nowe przepisy mogą wejść w życie jeszcze w tym roku.

Jakie zmiany wprowadza projekt znowelizowanej ustawy o KSC?

- Szerszy katalog objętych nią podmiotów: obok tradycyjnych sektorów, takich jak energia czy zdrowie, regulacje obejmą nowe obszary, np. produkcję chemikaliów, usługi pocztowe, sektor kosmiczny, a nawet wydobycie węgla.
- Samoocena i rejestracja: firmy będą musiały samodzielnie ocenić, czy są podmiotami kluczowymi lub ważnymi, i zarejestrować się w wykazie prowadzonym przez Ministra Cyfryzacji w ciągu 3 miesięcy od wejścia ustawy w życie. **UWAGA: nie dotyczy to podmiotów, które będą spełniać kryteria uznania za podmiot kluczowy lub ważny w momencie wejścia ustawy w życie. W przypadku tych podmiotów Minister Cyfryzacji opublikuje komunikat określający harmonogram złożenia wniosków o wpis do odpowiedniego wykazu. Przedsiębiorców telekomunikacyjnych, dostawców usług zaufania, podmioty publiczne i krytyczne Minister Cyfryzacji będzie sam wpisywał do tego wykazu i będą oni wzywani do uzupełnienia niektórych danych.**
- Audyt co 3 lata: w przeciwieństwie do poprzedniego wymogu audytów co 2 lata, nowy przepis wydłuża ten okres, dając firmom więcej czasu na dostosowanie. Pierwszy audyt będzie wymagany w ciągu 24 miesięcy.*
- Zmniejszenie kar dla kierownictwa podmiotów kluczowych lub ważnych: początkowo proponowano grzywny dla zarządów w wysokości 600% miesięcznego wynagrodzenia za naruszenia. Ostatecznie obniżono je do 300%, by złagodzić obawy przedsiębiorców.*
- Wzmocniony nadzór: Ministerstwo Cyfryzacji zyska prawo do przeprowadzania kontroli doraźnych, a procedury zgłaszania incydentów staną się bardziej precyzyjne.
- Ograniczenie sankcji: zawieszenie działalności będzie możliwe tylko w przypadku podmiotów kluczowych, co ma chronić mniejsze firmy przed nadmiernymi konsekwencjami.

*zmiany w najnowszym projekcie nowelizacji KSC z lutego 2025 r.

SEKTORY KLUCZOWE:

- Energetyka
- Ścieki
- Administracja publiczna
- Bankowość
- Transport
- Infrastruktura cyfrowa
- Przestrzeń kosmiczna
- Infrastruktura rynku finansowego
- Opieka zdrowotna
- Woda pitna
- Zarządzanie usługami ICT

SEKTORY WAŻNE:

- Usługi pocztowe i kurierskie
- Gospodarowanie odpadami
- Produkcja, wytwarzanie i dystrybucja chemikaliów
- Produkcja, wytwarzanie i dystrybucja żywności
- Produkcja
- Dostawcy usług cyfrowych
- Badania naukowe

DYREKTYWA NIS 2 WPROWADZA **3-STOPNIOWE RAPORTOWANIE**:

Wczesne ostrzeżenie

(early warning) – w ciągu 24 godz. wysłanie wczesnego ostrzeżenia, a tym samym ograniczenie rozprzestrzeniania incydentu.

Zgłoszenie incydentu

(notification) – w ciągu 72 godz. wstępna ocena skutków incydentu. Wyjątkiem są dostawcy usług zaufania, którzy mają na to 24 h zamiast 72 h.

Sprawozdanie końcowe

(final report) – nie później niż miesiąc po wstępnej ocenie przygotowanie szczegółowego raportu końcowego (tzw. lessons learned).

Sprawozdanie końcowe powinno zawierać:

- szczegółowy opis incydentu, w tym jego dotkliwość i skutki;
- rodzaj zagrożenia lub pierwotną przyczynę, która prawdopodobnie była źródłem incydentu;
- zastosowane i wdrażane środki ograniczające ryzyko na przyszłość;
- w stosownych przypadkach transgraniczne skutki incydentu.

7 KLUCZOWYCH ELEMENTÓW, KTÓRE MUSZĄ ZOSTAĆ UWZGLĘDNIONE PRZEZ ORGANIZACJĘ W CELU ZGODNOŚCI Z NIS2:

1. analiza ryzyka i polityki bezpieczeństwa systemów informacyjnych
2. ciągłość działania i zarządzania kryzysowego,
3. bezpieczeństwo łańcucha dostaw,
4. bezpieczeństwo pozyskiwania, rozwijania i utrzymywania sieci oraz systemów informacyjnych (w tym obsługi i ujawniania podatności),
5. polityka i procedury (testowanie i audyt) służące ocenie skuteczności środków zarządzania ryzykiem cyberbezpieczeństwa,
6. wykorzystywanie kryptografii i szyfrowania,
7. obsługa incydentów (zapobieganie, wykrywanie i reagowanie na incydenty).

Wczesne ostrzeżenie o incydencie poważnym, należy zgłosić w terminie **24 godzin od jego wykrycia** do CSIRT sektorowego. Zgłoszenie incydentu poważnego ma natomiast nastąpić w terminie **72 godzin od jego wykrycia**.

Progi incydentu poważnego

- Przerwanie ciągłości świadczenia usługi lub poważne obniżenie jakości usługi przez określony czas, dla określonej liczby użytkowników lub dla określonego obszaru geograficznego (dla każdej usługi progi będą określone odrębnie).
- Straty powyżej 500 tys. euro lub powyżej 5 proc. rocznego obrotu.
- Incydent spowodował ujawnienie tajemnicy przedsiębiorstwa.
- Incydent spowodował śmierć osoby.
- Incydent spowodował znaczny uszczerbek na zdrowiu.
- Miał miejsce skuteczny, prawdopodobnie złośliwy i nieuprawniony dostęp do sieci i systemów IT, który może spowodować poważna zakłócenia operacyjne.

KARY WEDŁUG PROJEKTU USTAWY O KSC:

Podmiot ważny:

Od **15 tys. zł** do **7 mln euro** lub **1,4%** łącznego rocznego światowego obrotu w poprzednim roku obrotowym przedsiębiorstwa

Podmiot kluczowy:

Od **20 tys. zł** do **10 mln euro** lub **2%** łącznego rocznego światowego obrotu w poprzednim roku obrotowym przedsiębiorstwa

Kary personalne:

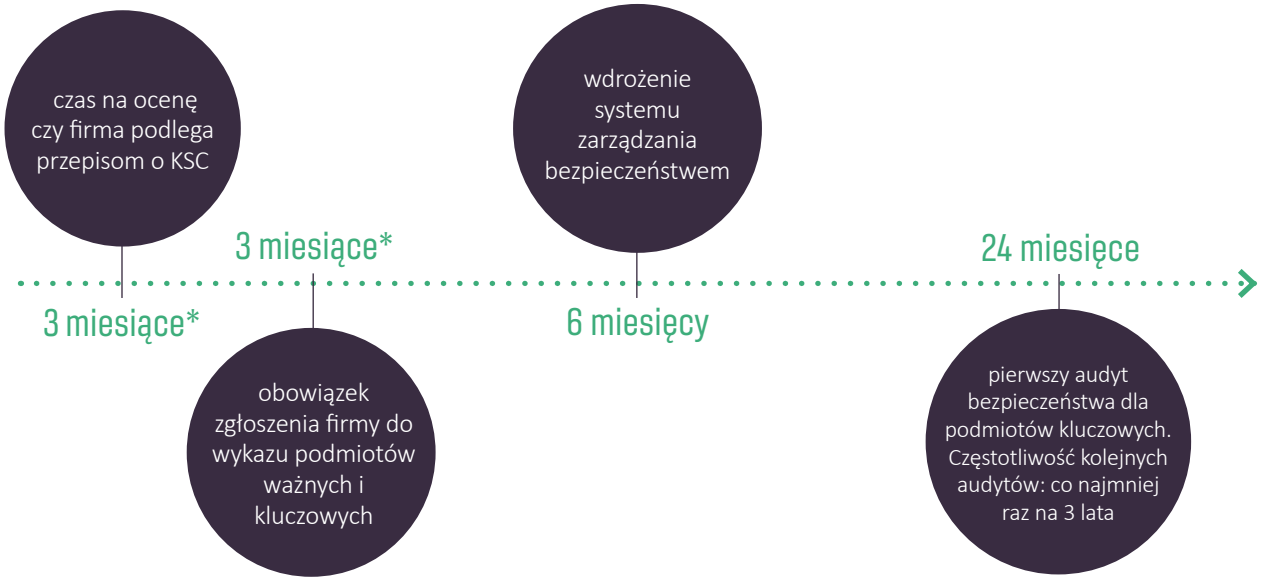
Niezależnie od kary nałożonej na spółkę, karę pieniężną można nałożyć również na kierownika podmiotu kluczowego lub podmiotu ważnego za niewykonanie obowiązków. Kierownik podmiotu kluczowego lub podmiotu ważnego ponosi odpowiedzialność także wtedy, gdy niektóre z obowiązków albo wszystkie obowiązki zostały powierzone innej osobie za jej zgodą.

Kara pieniężna może być wymierzona w kwocie nie większej niż 300% otrzymywanego przez ukaranego wynagrodzenia obliczonego według zasad obowiązujących przy ustalaniu ekwiwalentu pieniężnego za urlop.

Organ właściwy do spraw cyberbezpieczeństwa może zwrócić się do sądu o nałożenie tymczasowego zakazu zajmowania stanowiska przez osoby kierujące podmiotem kluczowym.

Inne sankcje:

- zawieszenie, ograniczenie zakresu albo cofnięcie koncesji do czasu gdy podmiot podejmie działania niezbędne do usunięcia uchybień lub zaprzestania naruszeń,
- wykreślenie podmiotu z rejestru działalności regulowanej,
- cofnięcie zezwolenia do czasu gdy podmiot podejmie działania niezbędne do usunięcia uchybień lub zaprzestania naruszeń,
- w celu przymuszenia do wykonania nałożonych obowiązków można nałożyć okresową karę pieniężną, w wysokości od 500 zł do 100 000 złotych za każdy dzień opóźnienia.



*Nie dotyczy to podmiotów, które będą spełniać kryteria uznania za podmiot kluczowy lub ważny w momencie wejścia ustawy w życie. W przypadku tych podmiotów Minister Cyfryzacji opublikuje komunikat określający harmonogram złożenia wniosków o wpis do odpowiedniego wykazu. Przedsiębiorców telekomunikacyjnych, dostawców usług zaufania, podmioty publiczne i krytyczne Minister Cyfryzacji będzie sam wpisywał do tego wykazu i będą oni wzywani do uzupełnienia niektórych danych.

Opracował M.J.

Wiele firm czeka organizacyjna rewolucja

Wielu przedsiębiorców wychodzi z założenia, że cyberbezpieczeństwo to jest po prostu koszt sprzętu i oprogramowania. Jednak w przypadku wdrażania przepisów transponujących dyrektywę NIS 2 takie podejście nie zadziała, bo ich sednem jest całościowa zmiana funkcjonowania organizacji, która ma doprowadzić do zapewnienia odpowiednio wysokiego poziomu cyberbezpieczeństwa. Dla niektórych z ISP największym wyzwaniem wcale nie będą więc kwestie związane z technologią, ale wprowadzenie odpowiedniej organizacyjnej dyscypliny i jej ścisłe przestrzegania – przestrzega Kinga Pawłowska-Nojszewska, radca prawny z Kancelarii Prawnej Media.

Czy przepisy nowelizowanej ustawy o Krajowym Systemie Cyberbezpieczeństwa będą trudne do wdrożenia dla operatorów telekomunikacyjnych i co może być w nich najbardziej problematyczne?

Moim zdaniem najtrudniejszą kwestią związaną z wdrażaniem nowych przepisów będzie konieczność dokonania zmiany całościowego funkcjonowania organizacji. Chcąc sprostać wprowadzonym wymaganiom nie wystarczy ograniczyć się do zakupu odpowiedniego programu do monitorowania systemu informacyjnego lub wynajęcia wyspecjalizowanego podmiotu, który będzie odpowiedzialny za cyberbezpieczeństwo. Nie mniej ważne będzie uporządkowanie funkcjonowania organizacji. Oznacza to też, że muszą powstać konkretne pakiety polityk i procedur związanych z zapewnieniem cyberbezpieczeństwa. Co więcej, obowiązkiem przedsiębiorców będzie przedstawianie dowodów na przestrzeganie tych procedur.

Jak to „tworzenie dowodów" ma wyglądać w praktyce?

Na przykład podczas kontroli, którą będą prowadziły UKE czy Ministerstwo Cyfryzacji, może paść żądanie pokazania logów z systemu wykorzystywanego do monitorowania świadczonych usług. Kontrolerzy mogą też zwrócić się o dowody, że personel jest szkolony z zakresu cyberhigieny, regularnie i adekwatnie do powierzonych mu obowiązków. To najprostsze przykłady, które jednak dobrze ilustrują, w jakim kierunku przedsiębiorcy będą musieli wprowadzać zmiany organizacyjne, by przekonać kontrolerów, że w ich firmach rzeczywiście procedury cyberbezpieczeństwa są przestrzegane. To jest właśnie – moim zdaniem – ta największa trudność, jaką przynosi NIS 2.

Czy te zmiany organizacyjne zawsze będą się musiały wiązać z zatrudnieniem dodatkowego pracownika, utworzeniem nowego działu, czy można będzie się oprzeć na zewnętrznych doradcach lub specjalistach?

Struktury odpowiedzialne za cyberbezpieczeństwo – czy to utworzone w organizacji, czy to zewnętrzne – będą musiały być wyodrębnione. W przypadku przedsiębiorców telekomunikacyjnych zatrudnianie zewnętrznych doradców na stałe nie musi być konieczne, ponieważ zapewnienie bezpieczeństwa sieci to w tym sektorze chleb powszedni. Można powiedzieć, że telekomy robią to od zawsze. Natomiast będzie musiało być jasne, kto za co odpowiada, jak odbywa się przekazywanie informacji, co zrobić „po kolei" w przypadku wystąpienia cyberincydentu. I oczywiście, wszystkie te kroki powinny mieć odwzorowanie w systemie informacyjnym, by potem wszystko można było łatwo sprawdzić i przeanalizować.

Czy to oznacza, że przedsiębiorcy telekomunikacyjni przy wdrażaniu NIS 2 są w trochę w lepszej sytuacji niż np. podmioty z sektora zdrowia, produkcji czy innych z branż, które będą podlegać przepisom znowelizowanej ustawy o KSC?

I tak, i nie. Bo skoro największym wyzwaniem jest wdrożenie nowej struktury organizacyjnej lub jej uporządkowanie, to akurat np. duże podmioty z sektora zdrowia są nawykłe do ścisłego przestrzegania procedur. Tam jest to czymś naturalnym. Natomiast u przedsiębiorców telekomunikacyjnych wiele zależy od tego, jak duży jest to pomiot i jak bardzo dbał o uporządkowanie funkcjonowania organizacji. A z tym jest różnie.

Bo choć u przedsiębiorców telekomunikacyjnych nacisk na to, żeby nie dochodziło do incydentów jest obecny od początku, to jest to tylko jeden ze składników w palecie nowych wymagań, jakie nałoży nowelizacja KSC. Dla niektórych z ISP największym wyzwaniem wcale więc nie będą kwestie związane z technologią, ale wprowadzenie odpowiedniej organizacyjnej dyscypliny i jej ścisłe przestrzeganie.

W sektorze telekomunikacyjnym w Polsce działa kilka tysięcy

Kinga Pawłowska-Nojszewska w rozmowie z **Ignacym Święcickim**, kierownikiem Zespołu Gospodarki Cyfrowej w Polskim Instytucie Ekonomicznym na konferencji KIKE (źr. TelkoIn)

Panel dyskusyjny na konferencji KIKE o nowelizacji ustawy KSC był bardzo emocjonujący. Na zdjęciu od lewej: prof. Ryszard Piotrowski, Uniwersytet Warszawski. Paweł Zegarow, kierownik Zespołu Strategii i Rozwoju Bezpieczeństwa Cyberprzestrzeni, Marcin Wysocki, Ministerstwo Cyfryzacji, Karol Skupień, prezes KIKE, Beata Kwiatkowska, Secfense, Kinga Pawłowska-Nojszewska, Kancelaria Prawna Media, Tomasz Bukowski, Kancelaria Prawna Media (źr. KIKE)

podmiotów, często są to firmy małe, a czasami mikrofirmy. Na ile są one dziś świadome zmian, jakie przyniesie nowelizacja ustawy o KSC i czy są do tego przygotowane?

Na pewno w branży każdy słyszał, że jest procedowana nowelizacja ustawy o KSC i wiąże się ona z wymogami w zakresie cyberbezpieczeństwa. Ta wiedza jest powszechna nawet wśród tych najmniejszych operatorów. Jedną z różnic między dużymi telekomami, a tymi najmniejszymi jest taka, że te pierwsze nie zastanawiają się nad tym, czy KSC ich dotknie czy nie, bo wiedzą, że będą objęci tymi regulacjami. Natomiast jeżeli chodzi o małe podmioty, to ciągle jest tu swego rodzaju niedowierzanie. Niemal na każdej konferencji czy zjeździe tego środowiska spotykam się z pytaniami ze strony małych przedsiębiorców, czy aby na pewno oni też będą podlegać tym przepisom. Co gorsza, niektórzy z nich żyją w przeświadczeniu, że gdy ustawa zostanie uchwalona, to sprawy tak się potoczą, że ostatecznie nie będą mieli jakichś szczególnych nowych obowiązków i nie będzie to dla nich oznaczać dużych zmian. Tu mogę ich jednak zapewnić, że akurat w tym zakresie dyrektywa NIS 2 jest dość precyzyjna i nie zostawia naszemu Ministerstwu Cyfryzacji zbyt dużego pola manewru. Wszyscy przedsiębiorcy telekomunikacyjni – niezależnie od wielkości – nowymi regułami z zakresu cyberbezpieczeństwa objęci zostaną na pewno. Pytanie tylko, czy jako podmioty kluczowe, czy ważne. To jest jedyna rzecz do rozstrzygnięcia.

Czy to oznacza, że małym operatorom będzie trudniej wdrażać regulacje NIS 2 niż dużym?

Wcale nie zakładałabym, że każdy duży telekom jest już dziś na pewno przygotowany do wejścia w życie znowelizowanej ustawy o KSC. Na pewno w lepszej pozycji wyjściowej są te podmioty, które mają zaimplementowane normy ISO 27001 i ISO 22301 dotyczące zarządzania systemami, które pomagają organizacjom chronić się przed zagrożeniami. ISO 27001 koncentruje się na bezpieczeństwie informacji, a ISO 22301 na ciągłości działania. Ta pierwsza jest bardziej powszechna w zastosowaniu. Jednak normy ISO stanowią jedynie wytyczne w zakresie sposobu działania, niezależnie od branży danego podmiotu. Samo wdrożenie ISO nie gwarantuje zgodności procedur z nowelizacją KSC, Prawem komunikacji elektronicznej, RODO, ustawą o zwalczaniu nadużyć w komunikacji elektronicznej itp.

Z reguły jest tak, że duża organizacja nie może sprawnie funkcjonować bez wprowadzenia pewnych procedur, w których ustalone są zakresy odpowiedzialności i określone działania. To może zaś sprawić, że łatwiej im będzie dostosować się do wymogów dyrektywy NIS 2. Wcale jednak nie zakładałabym, że każdy duży telekom jest już dziś na pewno przygotowany do wejścia w życie znowelizowanej ustawy o KSC. Na pewno w lepszej pozycji wyjściowej są te podmioty, które mają zaimplementowane normy ISO 27001 i ISO 22301 dotyczące zarządzania systemami, które pomagają organizacjom chronić się przed zagrożeniami. ISO 27001 koncentruje się na bezpieczeństwie informacji, a ISO 22301 na ciągłości działania. Ta pierwsza jest bardziej powszechna w zastosowaniu. Jednak normy ISO stanowią jedynie wytyczne w zakresie sposobu działania, niezależnie od branży danego podmiotu. Samo wdrożenie ISO nie gwarantuje zgodności procedur z nowelizacją KSC, Prawem komunikacji elektronicznej, RODO, ustawą o zwalczaniu nadużyć w komunikacji elektronicznej itp. W związku z powyższym duże czy średnie podmioty, nawet gdy wdrożyły u siebie obie normy ISO, powinny ustanowić strukturę odpowiedzialną za cyberbezpieczeństwo oraz ustanowić i wdrożyć procedury realizujące obowiązki wynikające z nowelizacji KSC.

Czy wdrożenie tych przepisów pociągnie za sobą koszty i jak duże mogą być one dla operatorów? Co będzie najkosztowniejsze przy wdrażaniu tych przepisów?

Wielu przedsiębiorców wychodzi z założenia, że cyberbezpieczeństwo to jest po prostu koszt sprzętu i oprogramowania. I mamy do wyboru drogie i tańsze rozwiązania, które można kupić i to załatwi problem. Jednak w przypadku NIS 2 to nie zadziała, bo sednem tych przepisów, co powtórzę jeszcze raz, jest zmiana całościowa funkcjonowania organizacji, która ma doprowadzić do zapewnienia odpowiednio wysokiego poziomu cyberbezpieczeństwa.

Najważniejsze jest więc to, aby organizacja wiedziała, jakie ma zasoby – ludzkie, sprzętowe, jakie ma oprogramowanie i odpowiednio do tego przygotowała analizę ryzyka. Dopiero na na podstawie tej analizy ryzyka, dana organizacja będzie mogła sobie dobrać droższe lub tańsze oprogramowanie. A może w wyniku analizy ryzyka dojdzie do wniosku – co będzie często dotyczyć zwłaszcza telekomów, które o cyberbezpieczeństwo dbały od zawsze – że nie musi nic nowego kupować, ponieważ odpowiednie zasoby już ma. To znaczy są one adekwatne do jego potrzeb, wielkości i skali zagrożeń. Dlatego też ponoszone koszty bardziej mogą wiązać się z zainwestowaniem w wiedzę czy analizy. To wszystko powoduje, że zaangażowanie kierownictwa jest kluczowe, by organizacja zaczęła działać zgodnie z tymi nowymi przepisami.

W związku z tym na pewno pojawią się koszty inwestycji w szkolenia pracowników, może też powstać konieczność zatrudnienia dodatkowej osoby. Zapewne w niejednym przypadku jakieś oprogramowanie też trzeba będzie kupić. Na pewno jednak skuteczność wdrożenia NIS 2 nie będzie można mierzyć kosztem tego czy ktoś kupił droższe czy tańsze oprogramowanie lub sprzęt. Chodzi o to, żeby świadomie analizować rzeczywiste potrzeby w tym zakresie i dopiero potem decydować o ewentualnych zakupach. Operatorzy i tak musieli inwestować w systemy zabezpieczające. Gros kosztów mogą więc w wielu przypadkach stanowić wydatki na analizy, stworzenie odpowiednich regulaminów czy zmiany organizacyjne.

Oczywiście konieczność monitorowania w trybie ciągłym

swojego systemu informacyjnego, wyznaczenie osoby, która rzeczywiście świadomie dba to cyberbezpieczeństwo w organizacji czy stworzenie odpowiednich procedur to też koszty, ale nie muszą być one wcale bardzo duże.

A kwestia raportowania incydentów?

Tu nie ma konieczności zakupu jakiegoś oddzielnego oprogramowania. NASK rozwija system S46, dostosowując go do wymogów nowelizacji ustawy o KSC. Docelowo wszyscy mają podłączyć się do tego systemu tworzonego przez NASK.

Obowiązek zapewnienia ciągłości działania operatorom też teoretycznie powinno być spełnić łatwiej niż podmiotom z innych branż?

Teoretycznie tak, ale tu jest też pewien haczyk. Zapewnienie ciągłości działania kojarzy się automatyczne z wykorzystywaniem narzędzi do tworzenia i zarządzania kopiami zapasowymi (backupami) i ich odzyskiwaniem po awarii, czy zadbaniem o odpowiedni poziom bezpieczeństwa w serwerowni (np. by spełniała przepisy przeciwpożarowe). Jednak w myśl przepisów nowelizowanej ustawy o KSC ciągłość działania dotyczyć będzie wszelkich ryzyk dla ciągłego i niezakłóconego świadczenia usług. Na ciągłość świadczenia usług mają wpływ nie tylko incydenty i awarie, lecz również m.in. straty finansowe, czy problemy kadrowe. Z tego powodu stworzenie systemu zarządzania ciągłością działania wymaga np. kontroli nad płynnością finansową i stworzenia planu działania nie tylko na wypadek pożaru czy powodzi, lecz na wypadek zatorów płatniczych. Musimy wiedzieć, jak długo jesteśmy w stanie świadczyć usługi w sposób ciągły gdy np. mamy problem ze ściąganiem należności od partnerów czy klientów.

Ministerstwo Cyfryzacji prezentując w październiku ub.r. finalną na tamten czas wersję projektu zapewniło, że udziela podmiotom wdrażającym te przepisy wsparcia finansowego. Wiadomo, że na taką pomoc mogły liczyć podmioty publiczne, samorządy. Czy operatorzy mogą też z jakichś źródeł o takie wsparcie się starać?

Na razie ja nie widzę tego typu programów dedykowanych dla operatorów, ani nawet ich zapowiedzi, tj. takich, które celowo zostały stworzone tylko po to, żeby dostosować się do nowych wymogów cyberbezpieczeństwa w organizacji. Można jednak szukać środków pośrednio, np. poprzez aplikowanie do programów na szeroko pojętą transformację cyfrową, gdzie być może przy okazji można sfinansować też przynajmniej część wydatków na cyberbezpieczeństwo. Na pewno można szukać też wsparcia na szkolenia pracowników, których jest akurat sporo i jeszcze na pewno będą ogłaszane.

Niektórzy uważają jednak, że wydatki związane z przystosowaniem się do wymogów znowelizowanego KSC należy traktować raczej jako inwestycję a nie koszt, bo będzie to procentować wzrostem poziomu cyberbezpieczeństwa. Może tak powinni podchodzić do tej kwestii operatorzy?

Trudno mi się do tego jednoznacznie ustosunkować. Mam jednak odczucie, że nie każdy przedsiębiorca telekomunikacyjny tak do tego podchodzi. Na pewno w ten sposób myślą podmioty, które zdecydowały się na wdrożenie wspomnianych wcześniej norm ISO związanych z cyberbezpieczeństwem. Jednak wielu mniejszych operatorów patrzy na to inaczej i dla nich te regulacje to kolejny przykry i niepotrzebny obowiązek. Argumentują, że przecież ich sieci, zawsze były, są i będą wystarczająco bezpieczne, więc to tylko niepotrzebna biurokracja.

Teraz jednak zapewnienie bezpieczeństwa sieci to tylko część zadania. Wymogiem będzie niezwłoczne podjęcie sprawnej wymiany informacji i współpracy z organami, szczególnie jeżeli dojdzie do incydentu poważnego lub odkryta zostanie poważna podatność w systemie, z którego korzystamy. Trzeba będzie być gotowym na szybką odpowiedź na pytanie: jakie zdarzenia kwalifikujemy jako incydenty? Kto jest odpowiedzialny za zgłaszanie incydentów i czy dysponuje odpowiednimi narzędziami, aby je wykrywać i oceniać według ważności? Z kolei jeżeli określona podatność spowodowała incydent u innego operatora, który korzysta z tego samego oprogramowania co my, możemy otrzymać szybko informację o istnieniu takiej podatności. Już zresztą dziś tak się często dzieje: NASK już teraz wysyła do przedsiębiorców informacje, że wykryto jakieś podatności. Po wejściu nowelizacji KSC w życie powinniśmy móc także odpowiedzieć jakie konkretnie kroki zostały podjęte w związku z informacją o podatności i kto był za to odpowiedzialny. Pewnie nie wszyscy mają wiarę i przekonanie, że wprowadzona wraz z nowelizacją ustawy o KSC „nowa biurokracja", czyli nowe procedury, są konieczne do podniesienia poziomu cyberbezpieczeństwa. Jednak wdrożenie takich procedur jest potrzebne, aby sprawnie reagować na cyberzagrożenia i cyberincydenty, a następnie – aby ocenić, czy dany skrypt postępowania warto zmienić, bo np. nie sprawdził się w praktyce.

Projektowana ustawa – co do tego chyba nie wątpliwości, obejmie wszystkich przedsiębiorców telekomunikacyjnych zarejestrowanych w UKE. Wyróżnia jednak dwie grupy podmiotów, które będą podlegać tym przepisom: podmioty kluczowe i ważne. Przepisy nowelizacji KSC przewidują, że przedsiębiorcy sami muszą rozstrzygnąć na zasadzie samooceny, do której grupy należą. Czy w tym zakresie mogą być wątpliwości, jak je rozstrzygnąć i jak mogą układać się proporcje między podmiotami ważnymi a kluczowymi w sektorze telekomunikacyjnym?

Pierwsza zasada jest taka, że podmiotem kluczowym będzie taki podmiot, który prowadzi działalność określoną w załączniku nr 1 do ustawy (czyli np. w sektorze infrastruktury cyfrowej) i zarazem jest większy niż średni. Z kolei podmiotem ważnym będzie podmiot, który prowadzi działalność określoną w załączniku nr 1 lub 2 do ustawy, kwalifikuje się jako średni przedsiębiorca, a jednocześnie nie jest podmiotem kluczowym w myśl tej pierwszej zasady. Od tych zasad istnieje jednak wiele wyjątków i takim wyjątkiem są m.in. przedsiębiorcy komunikacji elektronicznej. Przedsiębiorcy komunikacji elektronicznej będą kwalifikowani jako podmioty kluczowe już gdy będą przedsiębiorcami co najmniej średnimi, a jako podmioty ważne, gdy będą przedsiębiorcami mikro- lub małymi. Zatem rzeczywiście tak jest: wszyscy przedsiębiorcy komunikacji elektronicznej będą podlegać pod KSC, pytanie tylko czy jako podmiot kluczowy, czy ważny. Minister Cyfryzacji będzie wpisywać operatorów do wykazu podmiotów kluczowych i podmiotów ważnych z urzędu. Telekomy będą tylko deklarować swoją wielkość, tj., czy są mikro, małymi, średnimi czy dużymi przedsiębiorcami.

Należy przy tym zwrócić uwagę na kolejny wyjątek: wielu ISP świadczy również inne usługi, niż tylko usługi komunikacji elektronicznej. Dobrym przykładem są usługi DNS. Dostawca usług DNS jest podmiotem kluczowym bez względu na swoją wielkość. Nowelizacja KSC wprowadza zasadę, że gdy dany podmiot spełnia wymogi zarówno dla podmiotu kluczowego, jaki ważnego, jest podmiotem kluczowym. W związku z tym mikro- lub mały przedsiębiorca komunikacji elektronicznej, który jednocześnie świadczy usługę DNS, zostanie zakwalifikowany jako kluczowy.

W tym miejscu chciałabym również uczulić, że to nie ustawa – Prawo przedsiębiorców będzie służyła do oceny wielkości firmy, a unijne rozporządzenie w sprawie wyłączeń blokowych (tzw. rozporządzenie GBER). Dobrze znają je operatorzy, którzy ubiegali się do fundusze unijne. Zgodnie z tym rozporządzeniem, przy ocenie wielkości przedsiębiorcy należy wziąć pod uwagę liczbę personelu (przy czym liczbę personelu należy przeliczyć na liczbę „rocznych jednostek pracy") i rocznego obrotu – nie tylko własnego, lecz również u podmiotów powiązanych

i partnerskich. Dodatkowo niektórzy przedsiębiorcy przy ustalaniu wielkości firmy będą musieli uwzględnić partnerów B2B, z którymi stale współpracują. Tych przedsiębiorstw powiązanych i partnerskich nie trzeba będzie brać pod uwagę, jeżeli nasz system informacyjny będzie niezależny od systemów informacyjnych naszych przedsiębiorstw powiązanych, lub partnerskich lub nie świadczymy z nimi wspólnie usług.

Ustawodawca nie wskazał jasno, jakie kryteria należy spełnić, aby uznać, że dwa lub więcej podmiotów świadczy usługi wspólnie, ani które systemy informacyjne należy brać pod uwagę przy ocenie niezależności tych systemów. Wszystko to pokazuje, że kwestia liczby pracowników, którzy będą brani do określania wielkości firmy może być w niektórych przypadkach elementem szczegółowej analizy.

Czy rzeczywiście bycie podmiotem ważnym oznacza znacznie mniej obowiązków? A co jeśli ktoś będąc na granicy między podmiotem ważnym a kluczowym pomyli się w takiej samoocenie?

Na pewno przestrzegałabym, aby w takich sytuacjach granicznych „optymistycznie" nie kwalifikować się do grupy podmiotów ważnych, gdy nie mamy co do tego całkowitej pewności. Co prawda nie ma sankcji za nieprawdziwe oświadczenie jakiej wielkości jest się podmiotem. Jednak gdy w przyszłości kontrolerzy stwierdzą, że w istocie jesteśmy podmiotem kluczowym, a nie ważnym, skala kar może być ogromna z powodu zaniechań wykonywania obowiązków, jakie leżą na podmiotach kluczowych. Obowiązkiem, który spoczywa na podmiotach kluczowych, a na ważnych nie, jest cykliczny (przeprowadzany co trzy lata) audyt bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi. Taki audyt należy zlecić podmiotowi zewnętrznemu, a jego wyniki przesłać do organu, który przedsiębiorcę kontroluje. A minimalna kara za brak takiego audytu to dzisiaj 20 tys. zł.

Pierwszym obowiązkiem, który nowelizacja KSC nałoży na podmioty kluczowe i ważne jest wdrożenie systemu zarządzania bezpieczeństwem informacji (i ciągłości działania). Ten obowiązek jest taki sam w przypadku podmiotów kluczowych i ważnych, będących przedsiębiorcami, ale dobór konkretnych rozwiązań może być inny. System zarządzania bezpieczeństwem informacji powinien być proporcjonalny do oszacowanego ryzyka, z uwzględnieniem kosztów wdrożenia i wielkości podmiotu. Z kolei procedura zgłaszania incydentów będzie już identyczna w przypadku podmiotów kluczowych i ważnych. *De facto* jedyną różnicą w zakresie obowiązków, jest wspomniany już cykliczny audyt bezpieczeństwa systemu informacyjnego, bo na podmiotach ważnych ten obowiązek nie spoczywa. Można przy tym dodać, że podmioty mikro- i małe, niezależnie od tego, czy są podmiotami kluczowymi, czy ważnymi, będą musiały wyznaczyć jedną osobą odpowiedzialną za kontakty z innymi podmiotami kluczowymi i ważnymi. Podmioty większe będą zobowiązane do wyznaczenia dwóch takich osób.

Duże różnice pomiędzy podmiotami kluczowymi a ważnymi istnieją w skali kar pieniężnych oraz w zakresie środków nadzoru. Środki nadzoru są dość dotkliwe i dla jednej, i dla drugiej kategorii podmiotów, ale w przypadku podmiotów kluczowych katalog środków nadzoru jest znacznie szerszy. Przykładowo Prezes UKE może nakazać w drodze decyzji wykonanie przez przedsiębiorcę określonych konkretnych obowiązków we wskazanym przez ten organ terminie. W przypadku podmiotów kluczowych organ będzie mógł dodatkowo wyznaczyć w firmie urzędnika monitorującego, który będzie patrzył pracownikom na ręce, kiedy mają np. wyznaczony termin na doprowadzenie swojego systemu informatycznego do postawionych wymagań. Można więc sobie wyobrazić jak mało komfortowa to sytuacja, kiedy taki urzędnik monitorujący codziennie przychodzi do firmy i przygląda się, co tam się dzieje.

Inną istotną różnicą pomiędzy podmiotami kluczowymi a ważnymi jest przepis, który daje organowi kontrolnemu możliwość wydania nakazu wstrzymania prowadzenia działalności do czasu „usunięcia uchybień lub zaprzestania naruszeń". To jest najbardziej dotkliwy środek, bo w praktyce może oznaczać to koniec istnienia firmy.

W sektorze telko chyba największe kontrowersje wzbudzają przepisy o dostawcach wysokiego ryzyka (DWR). Jakie konsekwencje dla operatorów może mieć ich wdrożenie i czy naprawdę są tak groźne?

Samo w sobie wprowadzenie do ustawy instytucji prawnej dostawcy wysokiego ryzyka nie jest ani dobre, ani złe. Ważne jest to, jakie skutki będzie miało wdrożenie tego przepisu. I naszym zdaniem, w przypadku polskiej ustawy skutki te są tak daleko idące, jak w żadnym innym państwie UE. Pomijam już nawet fakt, że nie wszystkie kraje wdrożyły takie przepisy.
Ministerstwo Cyfryzacji wskazuje na konieczność zaimplementowania w Polsce tzw. 5G Toolbox, ale ten dokument dotyczy tylko dostawców sieci 5G i tylko elementów krytycznych w tych sieciach, które są jasno określone. Trudno więc zgadnąć dlaczego w Polsce te przepisy mają dotknąć aż 18 branż, które będą podlegać KSC.

Druga kwestia to: w oparciu o jakie kryteria definiować dostawców wysokiego ryzyka? Intuicyjnie, osoby nie zagłębione w tę dyskusję, mogą postrzegać tak firmy, które dostarczają wadliwy sprzęt czy oprogramowanie, które trzeba niezwłocznie naprawić lub usunąć ze swoich systemów. Na takie sytuacje już jednak istnieją inne, odpowiednie przepisy.

Na podstawie nowelizacji KSC za dostawcę wysokiego ryzyka można potencjalne uznać dowolnego dostawcę, w tym polskiego. Wiadomo jednak, że w przypadku KSC przepisy te powstały z myślą o dostawcach spoza UE, głównie chińskich. Nie wchodząc w dyskusję czy wprowadzenie wobec nich takiej procedury byłoby słuszne, powstaje jednak pytanie, czy adekwatny do rzeczywistego zagrożenia jest nakaz usunięcia całych kategorii sprzętu lub oprogramowania od takiego dostawcy. To oznacza wysokie koszty dla przedsiębiorców, których nikt im nie zrekompensuje. A przecież potencjalne ryzyko, nawet wysokie, można byłoby mitygować w inny sposób. Niezależnie od tych rozważań, wszystko wskazuje na to, że instytucja prawna dostawcy wysokiego ryzyka zostanie ujęta w nowelizacji KSC, w takim czy innym kształcie. Należy się zatem przygotować na możliwość pojawienia się decyzji DWR oraz uwzględnić ją w swojej polityce i procedurach bezpieczeństwa i ciągłości łańcucha dostaw.

Zostawiając na boku kontrowersje wokół DWR, w dyskusji nad nowelizacją KSC padają często argumenty o nadregulację też w zakresie innych przepisów. Czy są one słuszne i które z tych ewentualnych nadregulacji są najgroźniejsze?

Oprócz DWR, moim zdaniem, najbardziej dotkliwą nadregulacją jest możliwość nadania rygoru natychmiastowej wykonalności karom pieniężnym. O takim rygorze dyrektywa NIS 2 w ogóle nie wspomina, zatem jest to inwencja polskiego projektodawcy. Organ może nałożyć ten rygor „jeżeli wymaga tego ochrona bezpieczeństwa lub porządku publicznego". Oznacza to, że próg nadania rygoru natychmiastowej wykonalności takiej decyzji jest bardzo niski, bo przecież nawet zakłócenie ciszy nocnej może być traktowane jako naruszenie porządku publicznego. Naruszenie przepisów noweli KSC z definicji będzie naruszeniem porządku publicznego. Trudno ocenić, jakie względy powinny „uruchomić" rygor, więc w najgorszym scenariuszu może się potencjalnie okazać, że będzie on nakładany niemal za każdym razem, gdy dojdzie do naruszenia przepisów KSC. I co gorsza, rygor natychmiastowej wykonalności może być przeciwskuteczny, bo zamiast wydawać pieniądze na odpowiednie środki zapewnienia cyberbezpieczeństwa czy specjalistów, pierwszeństwo będzie miało natychmiastowe zapłacenie kary. W efekcie środków na to pierwsze może czasowo zabraknąć, co wcale nie poprawi sytuacji.
Kolejna sprawa to wprowadzenie polecenia zabezpieczającego,

które minister ds. informatyzacji będzie mógł wydać w razie wystąpienia incydentu krytycznego. Polecenie zabezpieczające w założeniu powinno doprowadzić do efektywnej i pilnej reakcji na taki incydent. Te obowiązki ujęte w poleceniu mogą być różne. Niektóre są w miarę oczywiste, jak np. zastosowanie konkretnej poprawki bezpieczeństwa, przeglądu procedur czy nakaz przeprowadzenia szacowania ryzyka związanego ze stosowaniem określonego produktu czy usługi. Teoretycznie chodzi o wprowadzenie środków ochrony proporcjonalnych do zidentyfikowanych ryzyk, ale niektóre mogą być bardzo dotkliwe, jak nakaz ograniczenia ruchu sieciowego przychodzącego od określonego podmiotu, który jest źródłem incydentu. Uciążliwość i zasadność tych rozwiązań będzie zależała od wielu dodatkowych zmiennych, które trudno dzisiaj przewidzieć. Trzeba jednak będzie przyjąć jakieś założenia i przygotować się na taki ewentualny scenariusz.

Tego typu nadregulacje w nowelizacji ustawy o KSC są punktowe, ale mogą mieć bardzo duże implikacje praktyczne. Z pewnością, jeżeli powyższe rozwiązania zostaną ujęte w nowelizacji KSC, trzeba będzie je uwzględnić w swoich analizach ryzyka i dokumentacji systemu zarządzania ciągłością działania.

Nowelizacja ustawy o KSC zobowiązuje wskazane podmioty także do przeprowadzenia analizy ryzyka. Co to oznacza dla operatorów telekomunikacyjnych?

To będzie podstawowa sprawa przy wdrażaniu tej ustawy. Tak naprawdę od tego trzeba zacząć, żeby najpierw ustalić, co w ogóle w organizacji mamy tj. jakie zasoby ludzkie, sprzętowe, software'owe, jakie procedury funkcjonują obecnie. Określenie tego będzie punktem wyjścia, który umożliwi stworzenie listy ryzyk dla bezpieczeństwa informacji i ciągłości świadczenia usług, a następnie podjęcie decyzji: czy dane ryzyko tolerujemy, czy jednak chcemy je znacznie ograniczyć? Na tym będzie właśnie polegać analiza ryzyka. Umożliwi ona adekwatną korektę istniejących procedur do nowych wymagań, by być w stanie odpowiednio reagować na incydenty i im zapobiegać.

Czy to będzie trudne? Zależy dla kogo, bo trzeba wiedzieć, jak to należy zrobić. Może to więc wiązać się z jakimś wydatkami np. na konsultacje, szkolenia, system monitorowania. Jest to jednak punkt wyjścia, który warunkuje prawidłowe spełnienie wszystkich innych kolejnych obowiązków.

Dlatego trzeba podkreślić, że taka analiza ryzyka jest niezwykle ważna. Dla operatorów telekomunikacyjnych oznacza to, że jeśli jej zaniechają, niczego dalej z KSC nie będą w stanie zrobić.

A czy wprowadzenie w nowelizacji ustawy o KSC kar bezpośrednio dla osób zarządzających daną organizacją to dobry pomysł, który będzie stymulował do działań podnoszących bezpieczeństwo operatorów i ich klientów?

Na pewno może być to rozwiązanie bardzo skuteczne, bowiem bez osób z zarządu i kierownictwa nie da się systemu bezpieczeństwa zaprogramować w taki sposób, żeby on był potem faktycznie egzekwowany i działał. Jednak moim zdaniem kary nie muszą być tak wysokie i powinny mieć bardziej charakter mobilizujący niż represyjny. A dziś można mówić o tym drugim, bowiem kara pieniężna może być wymierzona w kwocie do 300 proc. otrzymywanego przez ukaranego wynagrodzenia.

A czy zarząd firmy będzie mógł uniknąć tego zagrożenia i przenieść odpowiedzialność za funkcjonowanie procedur i systemu bezpieczeństwa na wynajętą w tym celu firmę czy specjalistę?

Można oczywiście umówić się na różne kary pieniężne z taką wynajętą firmą, ale w relacji z organem nie będzie możliwości przeniesienia odpowiedzialności. Jeden z członków zarządu musi być wyznaczony do zapewnienia przestrzegania przepisów ustawy. A jeżeli nie zostanie wskazany, będzie odpowiadał cały zarząd. Kierownik podmiotu kluczowego lub ważnego ponosi odpowiedzialność także wtedy, gdy niektóre z obowiązków albo wszystkie obowiązki zostały powierzone innej osobie za jej zgodą.

Jednym z najważniejszych obowiązków nakładanych przez procedowaną ustawę jest wdrożenie systemu zarządzania bezpieczeństwem informacji. Podmioty kluczowe i ważne będą musiały wyznaczyć osobę bądź osoby odpowiedzialne za utrzymywanie kontaktu z podmiotami Krajowego Systemu Cyberbezpieczeństwa (m.in. z Ministerstwem Cyfryzacji). Jak to się ma do RODO i czy to oznacza, że operatorzy będą musieli szukać takich specjalistów na rynku i ich wynajmować?

W każdej organizacji są przetwarzane różne informacje. W przypadku operatorów są to informacje o ruchu w sieci, ale i o klientach. Jeśli dojdzie do jakiegoś nietypowego lub nieprzewidzianego zdarzenia trzeba będzie ocenić jego znaczenie – czy był to incydent, czy też nie. Jeśli był to incydent, to czy trzeba będzie go zgłosić. Może się zdarzyć, że taki incydent ma związek z danymi osobowymi i wtedy trzeba wziąć pod uwagę też przepisy RODO. Dlatego też system zarządzania bezpieczeństwem informacji powinien być tak skonstruowany, żeby było jasne, w jakich sytuacjach pełnomocnik do spraw bezpieczeństwa informacji ma się także kontaktować z inspektorem ochrony danych osobowych (o ile firma wyznaczyła takiego inspektora), a kiedy nie musi.

Podmioty mają tu dowolność, jak tworzyć swoją strukturę organizacyjną. Jedna osoba może więc łączyć funkcję pełnomocnika ds. bezpieczeństwa informacji i inspektora ochrony danych osobowych. Funkcje te mogą być też rozdzielone. Można też wynająć specjalistę z zewnątrz. Ważne jest jednak, by mieć świadomość, że w pewnych sytuacjach wymogi z różnych aktów prawnych mogą się nakładać i RODO jest tu dobrym przykładem, ale nie jedynym. Wszystkie procedury telekomów powinny zostać tak skonstruowane, aby możliwie najsprawniej i bez niepotrzebnego mnożenia ról realizować obowiązki wynikające z nowelizacji ustawy o KSC, RODO, Prawa komunikacji elektronicznej, ustawy o zwalczaniu nadużyć w komunikacji elektronicznej, czy innych aktów prawnych. Do tego celu niezbędny jest m.in. sprawny przepływ informacji. Czyli podobnie jak w przypadku wielu innych obowiązków wynikających z przepisów prawa, konkretne rozwiązania służące zapewnieniu cyberbezpieczeństwa należy dobrać tak, aby zostały jak najlepiej dopasowane do struktur i potrzeb danej firmy.

Dziękujemy za rozmowę.
Rozmawiał Marek Jaślan

Kinga Pawłowska-Nojszewska

Radczyni prawna. Specjalistka w zakresie prawa cyberbezpieczeństwa.
Była autorką lub współautorką wielu stanowisk izb gospodarczych dotyczących cyberbezpieczeństwa oraz dobrze zna charakterystykę postępowań kontrolnych w tym zakresie.

W czasie wieloletniej współpracy z Kancelarią Prawną Media wspierała przedsiębiorców w postępowaniach przed Prezesem Urzędu Komunikacji Elektronicznej oraz w sporach z tym organem. Dzięki pracy w Urzędzie Komunikacji Elektronicznej oraz Ministerstwie Spraw Zagranicznych zyskała szeroką wiedzę w zakresie procesu legislacyjnego, zarówno polskiego, jak i unijnego, a także postępowań w zakresie naruszeń prawa unijnego.

KONTAKT:
tel. +48 533 552 334
kinga.pawlowska@kancelaria.media.pl

MEDIA
KANCELARIA PRAWNA

ZAPISZ SIĘ NA WEBINAR

Przedsiębiorca telekomunikacyjny, hostingodawca i szerzej: sektor infrastruktury cyfrowej. Od czego zacząć wdrażanie NIS2/KSC?

TOMASZ PROĆ

radca prawny
KANCELARIA PRAWNA MEDIA

KINGA-PAWŁOWSKA NOJSZEWSKA

radca prawny
KANCELARIA PRAWNA MEDIA

Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa zbliża się nieuchronnie, a wraz z nią nowe standardy związane z zapewnianiem bezpieczeństwa sieci. Czy naprawdę trzeba panikować?

Już 15.05 o godzinie 11:00 zapraszamy na webinar podczas którego, pokażemy Ci w praktyce:

✓Jak bez zbędnej teorii, krok po kroku i skutecznie wdrożyć NIS2/KSC w Twojej firmie?
✓Który program monitorujący (SIEM) jest najlepszy?
✓Jak działać, aby nowe przepisy były wsparciem, a nie tylko ciężarem?

15.05

11:00-12:30

MICROSOFT TEAMS

ZAPISZ SIĘ TUTAJ

Chmura może ułatwić dostosowanie do wymogów NIS2

Dla wielu podmiotów, które będą musiały spełnić wymogi z zakresu cyberbezpieczeństwa wprowadzone nowelizacją ustawy o KSC, a nie mają dziś u siebie odpowiednich zasobów, skorzystanie z usług dostawcy chmurowego może okazać się najlepszą opcją. I to zarówno organizacyjnie, jak i ze względu na przewidywalność kosztów – mówi **Marcin Lebiecki**, wiceprezes zarządu Asseco Cloud.

materiał powstał we współpracy z Asseco Cloud

Asseco podkreśla, że usługi Asseco Cloud są już dziś zgodne z dyrektywą NIS2. Co to oznacza? Czy jesteście pewni, że tym samym będziecie też automatycznie spełniać wymogi ciągle jeszcze nowelizowanej ustawy o Krajowym Systemie Cyberbezpieczeństwa, która ma implementować tę unijną dyrektywę na polski grunt?

Nie boimy się ani NIS2, ani nowelizacji ustawy o KSC. To wynika z naszego profilu i dziedzictwa. Jako Grupa Asseco funkcjonujemy w strategicznych sektorach, takich jak: finanse, zdrowie czy administracja publiczna. Wymusiło to na nas w sposób naturalny stworzenie odpowiednich komponentów technicznych do realizacji zadań najbardziej wymagających pod względem bezpieczeństwa i ciągłości działania. Przepisy NIS2 nie są więc dla nas żadną nowością, a codziennością, biorąc pod uwagę wymogi klientów, z którymi pracujemy.

Jednym z zasadniczych komponentów naszej oferty jest konsulting i doradztwo – staramy się dobrze zrozumieć, jakie potrzeby ma każdy klient, czym dysponuje, by w jak najlepszy sposób podejść do projektu, który będziemy u niego realizowali. A potem odpowiednio dostosować do tego elementy techniczne i opracować procesy. To w dużej mierze działania, jakie będzie trzeba podejmować wdrażając przepisy NIS2.

Podsumowując przez lata wytworzyliśmy różne komponenty naszych usług związanych z cyberbezpieczeństwem. Posiadamy własną infrastrukturę, silne kompetencje i doświadczony zespół managed services (usług zarządzanych), który pracuje na co dzień z klientami i wspiera ich działy IT.

Sektor IT jako całość z pewnością skorzysta na wdrożeniu dyrektywy NIS2 – ocenia **Marcin Lebiecki**, wiceprezes zarządu Asseco Cloud (źr. Asseco)

Czy perspektywa dostosowania się do wymogów NIS2, a w Polsce ustawy KSC wpływa na zainteresowanie waszymi usługami?

Zdecydowanie tak. Wcześniej naszą ofertą interesowali się głównie duzi klienci i to w projektach u nich realizowanych wykorzystywaliśmy nasz potencjał. Teraz zaczynają docierać do nas z zapytaniami nowe, także mniejsze, jeśli chodzi o skalę działania, firmy i organizacje. Bardzo często właśnie z powodu konieczności dostosowania się do dyrektywy NIS2.

Traktujemy to jako szansę rynkową. Ta grupa klientów nie szuka wprost rozwiązania chmurowego, ale bardziej partnera, który ich przeprowadzi przez cały proces dostosowywania się do wymogów NIS2. Zresztą my sami siebie też nie postrzegamy, jako typowego dostawcy technologii chmury „takiej czy innej", ale staramy się być dla naszych klientów partnerem technologicznym, który ma wszystkie niezbędne komponenty do tego, by – w tym przypadku – dana organizacja mogła w sposób optymalny i jak najmniej uciążliwy, dostosować się do wymogów NIS2.

Czy można więc stwierdzić, że dyrektywa NIS2 pozytywnie wpłynie na rozwój usług chmurowych w Polsce i cały sektor IT?

Na rynku w różnych okresach można dostrzec fascynację różnymi technologiami w różnych okresach, które mają stać się akceleratorem dla wzrostu efektywności całej gospodarki. Parę lat temu taką technologią była chmura, dziś jest nią AI. W przypadku chmury wiele prognoz się sprawdziło, ale też oczekiwania były większe. Implementacja każdej technologii napotyka na różnego rodzaju bariery. Jedną z nich są ograniczenia finansowe, które sprawiają, że wiele firm odsuwa w czasie transformację cyfrową, bo ważniejsze w ich przypadku są inne cele biznesowe.

A wymagania prawne zmuszą teraz wiele podmiotów, by podjąć konkretne działania w obszarze cyberbezpieczeństwa. Dużo firm, które staną się podmiotami kluczowymi lub ważnymi nie ma odpowiednich zasobów – czy to technicznych czy ludzkich, by samodzielnie sprostać wymaganiom NIS 2. Skorzystanie z usług dostawcy chmurowego wydaje się więc

sensownym rozwiązaniem, a dla wielu podmiotów zapewne jedynym, gdy np. będą chciały mieć gwarancję ciągłości usług. To zaś może sprawić, że gdy w średnim lub dłuższym okresie zaczną odczuwać korzyści ze współpracy z dostawcami chmurowymi, sięgną po inne oferowane przez nich usługi i zdecydują się na zrobienie kolejnego kroku na drodze do transformacji cyfrowej.

Sektor IT jako całość z pewnością skorzysta na wdrożeniu dyrektywy NIS2. Wierzę jednak, że również organizacje, które będą implementować wymagane rozwiązania, szybko dostrzegą, że była to inwestycja z sensem, przynosząca długofalowe korzyści. W rezultacie jeszcze chętniej otworzą się na cyfryzację. Właśnie temat cyberbezpieczeństwa, rozwiązań chmurowych i korzyści płynących z inwestowania w technologię poruszę podczas konferencji Impact'25 w Poznaniu, podkreślając, że budując odporność cyfrową dziś, tworzymy bezpieczniejszą i bardziej konkurencyjną gospodarkę jutra.

W jakim stopniu korzystanie z usług chmurowych może ułatwić dostosowanie się do wymogów nowelizowanej ustawy o KSC?

To zależy od sytuacji, w jakiej znajduje się konkretna organizacja. Nie jest tajemnicą, że wiele przedsiębiorstw w Polsce jest niedoinwestowanych, jeśli chodzi o rozwiązania i technologie z obszaru cyberbezpieczeństwa. Należy odpowiedzieć na pytania - czy będziemy w stanie szybko zbudować takie zasoby? Zdobyć odpowiednie kompetencje i znaleźć specjalistów? Jakim kosztem to nastąpi? W tej sytuacji dla wielu podmiotów, które będą musiały spełnić wymogi z zakresu cyberbezpieczeństwa narzucone przez ustawę o KSC, skorzystanie z usług dostawcy chmurowego może być najlepszą opcją. I to zarówno organizacyjnie, jak i ze względu na przewidywalność kosztów. A także w kontekście tego, jakie dodatkowe rozwiązania, nie tylko z zakresu cyberbezpieczeństwa, może w przyszłości zapewnić taki chmurowy partner.

Dziękujemy za rozmowę.
Rozmawiał Marek Jaślan

materiał powstał we współpracy z Asseco Cloud

UKE będzie miał 1,5 roku na zbudowanie sektorowego CSIRT-u

Projekt nowelizacji ustawy o KSC przewiduje m.in., że Prezes UKE ma zbudować i prowadzić sektorowy Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT) dla podsektora komunikacji elektronicznej i sektora usług pocztowych. Dla operatorów oznacza to, że regulator będzie przeprowadzać ocenę bezpieczeństwa ich systemów IT, oraz że będą mu raportować cyberincdynety.

Wejście w życie nowelizowanej ustawy o KSC oznacza też nowe obowiązki dla Urzędu Komunikacji Elektronicznej. I to nie tylko dlatego, że regulator rynku telekomunikacyjnego stanie się podmiotem kluczowym w sektorze instytucji publicznych.

Zgodnie bowiem z projektem nowelizacji ustawy o KSC (wg projektu z 7.02.2025 r.) Prezes UKE będzie organem właściwym ds. cyberbezpieczeństwa dla podsektora komunikacji elektronicznej i sektora usług pocztowych, a także ma prowadzić CSIRT sektorowy (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, ang. Computer Security Incident Response Team) dla podsektora komunikacji elektronicznej i sektora usług pocztowych.

Dla operatorów telekomunikacyjnych i pocztowych oznacza to, że to UKE będzie sprawdzał czy spełniają one wymogi KSC, a do sektorowego CSIRT-u UKE będą zgłaszać cyberincydenty.

Czy zadania CSIRT UKE nie będą nachodziły lub kolidowały z CSIRT NASK?

– *Architektura krajowego systemu cyberbezpieczeństwa uwzględniająca CSIRT-y sektorowe zapewnia swoiste odciążenie CSIRT-ów poziomu krajowego przy jednoczesnym lepszym dopasowaniu merytorycznym do specyfiki danego sektora. Nie przewiduje się kolizji w zakresie kompetencji, a wzajemne uzupełnianie – odpowiada Witold Tomaszewski, rzecznik UKE*

W związku z tym Prezes UKE, który ma otrzymać środki aż na 54 nowe etaty (40 na komunikację elektroniczną i 14 na pocztę) z tytułu nadzoru nad komunikacją elektroniczną oraz nad pocztą (40 etatów to maksymalny pułap wzrostu zatrudnienia na jeden obszar).

W ocenie skutków regulacji nowelizacji KSC oszacowano roczny koszt funkcjonowania CSIRT sektorowego na kwotę ponad 8,2 mln zł z zastrzeżeniem, że należy ją traktować jako maksymalną. Wydatki na utworzenie i funkcjonowanie CSIRT-ów sektorowych mają zostać poniesione przez budżet państwa.

Jednak z rekrutacją na etaty do swego CSIRT UKE musi się wstrzymać dopóki

ostateczna wersja ustawy nie zostanie przyjęta i nie wejdzie w życie. Na obecnym etapie jedyne co może robić i robi regulator w związku z ustawą o KSC, to bieżąca analiza kolejnych jej projektów, szczególnie pod kątem przewidzianych przyszłych zadań, które mogą mu przypaść.

Na uruchomienie sektorowego CSIRT, UKE będzie miał półtora roku, bowiem procedowany projekt ustawy przewiduje osiągnięcie pełnej gotowości przez CSIRT sektorowy w terminie do 18 miesięcy od dnia wejścia jej w życie.
UKE zastrzega, że w chwili obecnej trudno jest określić szczegółową liczbę podmiotów kluczowych i podmiotów ważnych, które znajdą się w jego orbicie. Jednak na podstawie rejestrów RPT, ROP (rejestry przedsiębiorców telekomunikacyjnych i operatorów pocztowych) oraz szacunków dotyczących podmiotów świadczących publicznie dostępne usługi komunikacji interpersonalnej niewykorzystujących numerów, można wstępnie założyć, że łączna ich liczba będzie wynosiła ok. 4 tys.

Na obecnym etapie UKE nie chce oceniać, z jakimi wymogami przy wdrażaniu wymogów ustawy o KSC mogą mieć największe kłopoty operatorzy telekomunikacyjni i pocztowi.

– *Stopień trudności realizacji obowiązków nakładanych na podmioty kluczowe i podmioty ważne, sygnalizowanych w kolejnych projektach nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa, zależy od indywidualnego stopnia dojrzałości w podejściu do cyberbezpieczeństwa każdego z tych podmiotów, dlatego to one powinny być adresatami takiego pytania* – mówi rzecznik UKE.

Na obecnym etapie jedyne co może robić i robi UKE w związku z ustawą o KSC, to bieżące dokonywanie szczegółowych analiz jej kolejnych projektów (Źr.UKE)

Dla UKE stworzenie od podstaw sektorowego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego sektorowego CSIRT, to w pewnym sensie wejście na terra incognita. Okres 18 miesięcy w tym przypadku wcale nie wydają się być długi, tym bardziej, że odpowiedniej klasy specjalistów od cyberbezpieczeństwa wcale nie jest tak łatwo pozyskać na rynku. A zadania stojące przed CSIRT-em sektorowym wcale nie są banalne. I tak np. podmiot kluczowy lub ważny będzie zgłaszał do niego wczesne ostrzeżenie o incydencie poważnym (24 godziny od momentu wykrycia), kolejnym krokiem będzie zgłoszenie incydentu poważnego (72 godziny od momentu wykrycia). Zgłoszenie wczesnego ostrzeżenia może zawierać wniosek o wskazanie wytycznych dotyczących możliwych do wdrożenia środków ograniczających skutki incydentu poważnego lub o wsparcie techniczne przy obsłudze incydentu. CSIRT sektorowy zobowiązany będzie w terminie 24 godzin udzielić wsparcia zgodnie z treścią wniosku.

Można mieć tylko nadzieję, że realizacja tego zadania pójdzie urzędowi lepiej niż budowa Punktu Informacyjnego ds. Telekomunikacji (PIT), gdzie operatorzy muszą m.in. raportować swe dane o infrastrukturze. Będzie to zresztą zadanie, które najpewniej spadnie już na barki nowego prezesa UKE, bowiem 18 września br. kończy się pięcioletnia kadencja obecnego szefa regulatora – dr. inż. Jacka Oko.

Marek Jaślan

CO NA RYNKU ICT ZMIENIA NOWELIZACJA USTAWY O KSC?

SAYF materiał partnera

Przepisy dyrektywy UE skierowane są do rządów państw członkowskich i powinny być wdrożone do krajowego systemu prawnego i dopiero wtedy będą obowiązywały w tym kraju członkowskim. Do polskiego prawa przepisy te wdrażane są ustawą o zmianie ustawy o Krajowym Systemie Cyberbezpieczeństwa.

Pamiętać należy, że na podstawie Dyrektywy NIS2 wydano kilka rozporządzeń, które nie wymagają transpozycji do krajowego systemu prawnego i należy stosować je bezpośrednio, np. znane przez wiele podmiotów rozporządzenie DORA.

Tytuł Dyrektywy NIS2 oraz potoczny przekaz sugerują, że przepisami tej dyrektywy i przepisami wydanymi na jej podstawie objęte będą zagadnienia wyłącznie ograniczone do cyberprzestrzeni.

Pragniemy wyjaśnić, że ochroną w sposób i na zasadach określonych w przepisach wydanych na podstawie Dyrektywy NIS 2 objęte będą wszelkie informacje mające nawet najmniejsze znaczenie w przedsiębiorstwie, urzędzie, instytucji.

Z treści NIS2, projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw wynika, że ochrona musi dotyczyć wielu obszarów i aspektów ochrony, przy czym nie ulega wątpliwości, że najważniejsze działanie będzie dotyczyć bezpieczeństwa informacji przetwarzanej w systemie teleinformatycznym.

Wejście w życie Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającej rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) bardzo poważnie zmieni podejście wielu podmiotów do zagadnień związanych z ochroną informacji.

O tym, jak przygotować się do realizacji obowiązków związanych z wejściem w życie Dyrektywy NIS, specjaliści z SayF wyjaśniali m.in. na ostatniej konferencji KIKE. (źr. SayF)

Co zmienia wejście w życie przepisów wydanych na podstawie dyrektywy NIS2?

Przepisy wydane na podstawie Dyrektywy NIS2 wprowadzają bardzo istotne obowiązki lub powinności, w tym:

- obowiązek zgłoszenia do rejestru podmiotów podlegających obowiązkom określonym w ustawie o KSC, prowadzonego przez wyznaczony organ administracji rządowej. Przedsiębiorcy wpisani do Rejestru Przedsiębiorców Telekomunikacyjnych prowadzonego przez Prezesa UKE z urzędu zostaną wpisani do wykazu podmiotów kluczowych i ważnych,
- bezpośrednia odpowiedzialność osób kierujących przedsiębiorstwem za zapewnienie bezpieczeństwa na odpowiednio wysokim poziomie,
- wymóg opracowania, wdrożenia, stosowania i aktualizacji dokumentów opisujących realizację obowiązków zapewnienia bezpieczeństwa informacji. Obowiązek przechowywania przez co najmniej dwa lata kalendarzowe ww. dokumentacji wycofanej z użytkowania, a brakowanie tej dokumentacji musi być potwierdzone protokołem specjalnie wyznaczonej do tego komisji,
- audyty wypełniania obowiązków wynikających z Dyrektywy NIS2 bezpieczeństwa informacji – obowiązkowe, cykliczne wobec podmiotów kluczowych oraz doraźnie wobec pozostałych podmiotów, oraz raportowanie wyników audytu do organu nadzorczego w sprawach cyberbezpieczeństwa,
- prawo podmiotów korzystających z usług ICT do częściowego lub pełnego audytu podmiotów świadczących takie usługi.

Z namiastką kontroli realizacji obowiązków z zakresu cyberbezpieczeństwa przez usługobiorców usług ICT spotkali się przedsiębiorcy telekomunikacyjni świadczący usługi na rzecz instytucji finansowej. Instytucje finansowe oraz dostawcy usług ICT obowiązani są przestrzegać zasad określonych w rozporządzeniu DORA, które obowiązuje od 17 stycznia 2025 r. Wiele telekomów zostało już „uszczęśliwionych" nowymi umowami lub aneksami do umów świadczenia usług na rzecz podmiotów finansowych. Organy nadzorcze będą miały bardzo dużo informacji o wykonywaniu przez przedsiębiorców obowiązków z zakresu cyberbezpieczeństwa bez konieczności podejmowania jakichkolwiek działań.

Tylko te przytoczone wyżej argumenty wskazują, że obowiązki wynikające z NIS2 muszą być wykonywane począwszy od dnia wejścia w życie tych przepisów oraz w profesjonalny sposób.

Nie da się wykonać tych obowiązków ad hoc, np. w związku ze zbliżającym się audytem lub kontrolą upoważnionego organu. Rolę kontrolerów pełnić będą podmioty korzystające z usług zewnętrznych dostawców usług ICT lub audytorzy oceniający zgodność realizowanych obowiązków z przepisami prawa powszechnego.

Właśnie te mechanizmy „kontroli" powodujące nieuchronność realizacji opisywanych obowiązków, w naszej ocenie, są najistotniejszymi zmianami wprowadzanymi przepisami wydanymi na podstawie Dyrektywy NIS2.

Andrzej Fudala, Dariusz Fudala
Specjaliści do spraw ochrony informacji. Audytorzy wiodący systemu zarządzania bezpieczeństwem wg normy PN-EN 27001

Jak będzie przebiegać procedura uznania za dostawcę wysokiego ryzyka?

Jednym z najbardziej kontrowersyjnych rozwiązań, które ma wprowadzić nowelizowana ustawa o KSC są projektowane zapisy o dostawcach wysokiego ryzyka (DWR). Mają one sprawić, że niebezpieczny sprzęt i usługi będą eliminowane z użycia w kluczowych dla funkcjonowania państwa systemów teleinformatycznych.

Proces uznania dostawcy za dostawcę wysokiego ryzyka oraz związane z tym obowiązki, takie jak natychmiastowe wstrzymanie korzystania z produktów DWR, ich wycofanie oraz zakaz nabywania w ramach zamówień publicznych, mogą w przyszłości stanowić istotne wyzwanie dla niektórych przedsiębiorców. Tym bardziej, że w tym kontekście w dyskusjach najczęściej mówi się o firmach chińskich, takie jak Huawei czy ZTE, których dotknąć mogłyby tego rodzaju sankcje. Tymczasem technologie tych firm są dość szeroko wykorzystywane w polskich firmach ze względu na ich konkurencyjność cenową, a wielu przekonuje, że są też bardzo dobre pod względem technologicznym. **Związek Telewizji Kablowych w Polsce Izba Gospodarcza (ZTKiG)** w swoim stanowisku do Ministerstwa Cyfryzacji odnośnie zapisów o DWR w nowelizowanej ustawie o KSC, posunął się nawet do stwierdzenia, że sprzęt wyprodukowany przez Huawei w CHRL, którego od wielu lat używa wielu operatorów, jest „niezawodny", „bezawaryjny" lub „o bardzo niskiej awaryjności" w porównaniu z urządzeniami i oprogramowaniem produkowanymi w Unii Europejskiej czy Polsce. To ostatnie stwierdzenie spotkało się z ostrym sprzeciwem i oburzeniem niektórych producentów z Polski.

W naszym raporcie do kontrowersji związanych z zapisami o DWR odnoszą się w wywiadach Kinga Pawłowska-Nojszewska, radca prawny w Kancelarii Prawnej Media, oraz Marcin Wysocki, zastępca dyrektora Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji,

Procedura uznania dostawcy za DWR może zostać wszczęta z urzędu przez Ministra Cyfryzacji lub na wniosek przewodniczącego Kolegium ds. Cyberbezpieczeństwa. Postępowanie dotyczyć zaś będzie dostawców sprzętu lub oprogramowania, którzy zaopatrują podmioty kluczowe lub ważne.

Resort cyfryzacji podkreśla przy tym, że decyzje tego typu będą wynikiem wieloetapowego postępowania, w którym uczestniczyć będzie Kolegium ds. Cyberbezpieczeństwa oraz fakultatywnie, organizacje społeczne i Prezes UOKiK. Jak bowiem przewidują proponowane przepisy, przed podjęciem decyzji przez Ministra Cyfryzacji, Kolegium ds. Cyberbezpieczeństwa musi wydać opinię, która zawierać ma analizę ryzyka wynikającego z dalszej współpracy z danym dostawcą. Analiza obejmować będzie zagrożenia związane z bezpieczeństwem narodowym, zagrożenia ekonomiczne, wywiadowcze, czy terrorystyczne.

Ministerstwo Cyfryzacji zwraca też uwagę, że decyzja będzie uwzględniać indywidualną sytuację przedsiębiorcy, biorąc pod uwagę zarówno przesłanki prawno-polityczne (ryzyko stworzenia zagrożeń) jak i techniczne, takie jak liczba i rodzaj wykrytych podatności i incydentów, tryb i zakres w jakim dostawca sprawuje nadzór nad procesem wytwarzania. Przy czym uznanie dostawcy za dostawcę wysokiego ryzyka ma odbywać się w drodze postępowania administracyjnego, dotyczącego konkretnego podmiotu, a nie wszystkich dostawców z danego kraju.

Po uzyskaniu opinii Kolegium ds. Cyberbezpieczeństwa, Minister Cyfryzacji podejmuje decyzję o uznaniu dostawcy za DWR. Decyzje będą publikowane w dzienniku urzędowym „Monitor Polski" i będą podlegać natychmiastowemu wykonaniu. Oznacza to, że podmioty kluczowe i ważne będą miały obowiązek przystąpić do ich realizacji niezwłocznie. A to oznacza, że od ogłoszeniu decyzji, podmioty korzystające z produktów dostawcy uznanego za DWR będą musiały:

- natychmiast wstrzymać wprowadzanie do użytkowania sprzętu, oprogramowania lub usług od dostawcy uznanego za DWR,
- wycofać z użytkowania te produkty w ciągu 7 lat od wydania decyzji (4 lata w przypadku krytycznych funkcji ICT),
- wstrzymać zakupy produktów od dostawcy DWR w ramach zamówień publicznych.

Decyzja o uznaniu dostawcy za dostawcę wysokiego ryzyka będzie zaskarżalna do sądu administracyjnego, co – w ocenie resortu cyfryzacji – zapewnia obiektywne i niezależne spojrzenie na sprawę.

Opracował M.J.

Schemat postępowania uznania za Dostawców wysokiego ryzyka

01	Wszczęcie postępowania przez ministra właściwego ds. informatyzacji	z urzędu	na wiosek przewodniczącego Kolegium do Spraw Cyberbezpieczeństwa
02	Zawiadomienie o wszczęciu postępowania	Strony postępowania	Prokurator Generalny
03	Opublikowanie informacji o wszczęciu postępowania w BIP właściwego ministra	Niezwłocznie po doręczeniu zawiadomienia	W przypadku strony z siedzibą poza UE, Szwajcarią, EFTA albo EOG – udostępnienie zwiadomienia w BIP po 14 dniach ma skutki identyczne jak doręczenie
04	Przedstawienie stanowisk przez organizacje społeczne	Fakultatywnie w terminie 14 dni od opublikowania informacji	Minister właściwy do spraw informatyzacji publikuje w BIP raport ze złożonych w terminie stanowisk, wskazując w szczególności główne uwagi zawarte w stanowiskach
05	Zasięgnięcie opinii Kolegium do Spraw Cyberbezpieczeństwa	Termin na dostarczenie opinii: 3 miesiące	Przygotowuje zespół opiniujący powoływany przez przewodniczącego Kolegium, w jego skład może wejść także przedstawiciel Prezesa UOKiK
06	Wydanie decyzji o uznaniu za dostawcę wysokiego ryzyka	Dotyczy dostawcy sprzętu i oprogramowania oraz podmiotów wchodzących w skład grupy kapitałowej	Wydawana przez ministra właściwego ds. informatyzacji Obowiązek wycofania dotyczy wyłącznie typów sprzętu i oprogramowania wskazanych w decyzji
07	Ogłoszenie decyzji w Dzienniku Urzędowym „Monitor Polski" oraz udostępnienie w BIP i na stronie internetowej urzędu obsługującego właściwego ministra		
08	Wykonanie decyzji co do typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT dostarczanych przez dostawcę wysokiego ryzyka i wskazanych w decyzji		
09	Kontrola wykonania decyzji w sprawie uznania za dostawcę wysokiego ryzyka	Organy właściwe ds. cyberbezpieczeństwa	Podmioty kluczowe i ważne obowiązkowo przekazują informacje o wycofywanych produktach, procesach i usługach na wniosek organów właściwych

Strony postępowania ws. uznania za DWR

- każdy wobec kogo zostało wszczęte postępowanie
- fakultatywnie na prawach strony także przedsiębiorca telekomunikacyjny, spełniający określone ustawowo warunki
  - ma siedzibę na terytorium Polski
  - wpisany do rejestru przedsiębiorców telekomunikacyjnych
  - w poprzednim roku obrotowym (roku przed którym wszczęto postępowanie) uzyskał przychód z tytułu działalności telekomunikacyjnej w wysokości co najmniej dwudziestotysięcznej krotności przeciętnego wynagrodzenia wskazanej w ostatnim ogłoszonym przed wszczęciem postępowania komunikacie Prezesa GUS

Opinia Kolegium do Spraw Cyberbezpieczeństwa zawiera analizy:

- zzagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, wywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi dostawca,
  - z uwzględnieniem informacji o zagrożeniach uzyskanych od państw lub organów UE lub NATO
- prawdopodobieństwa z jakim dostawca znajduje się pod kontrolą państwa spoza terytorium UE lub NATO, z uwzględnieniem:
  - przepisów prawa regulujących stosunki między dostawcą, a tym państwem oraz praktyki stosowania prawa w tym zakresie,
  - prawodawstwa oraz stosowania prawa w zakresie ochrony danych osobowych, w szczególności, gdy nie ma porozumień w tym zakresie między UE i tym państwem,
  - struktury własnościowej dostawcy,
  - zdolności ingerencji tego państwa w swobodę działalności gospodarczej dostawcy;
- powiązań z podmiotami określonymi w załączniku I do rozporządzenia Rady (UE) 2019/796
- liczby i rodzajów wykrytych podatności i incydentów dotyczących typów produktów lub rodzajów usług lub konkretnych procesów ICT dostarczanych przez dostawcę oraz sposobu i czasu ich eliminowania;
- trybu i zakresu, w jakim dostawca sprawuje nadzór nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania dla wskazanych w ustawie podmiotów, oraz ryzyka dla procesu wytwarzania i dostarczania sprzętu lub oprogramowania;
- treści wydanych w wyniku badania podatności na gruncie ustawy rekomendacji Pełnomocnika ds. Cyberbezpieczeństwa, dotyczących sprzętu lub oprogramowania danego dostawcy.

Decyzja o uznaniu za DWR

- W szczególności zawiera wskazanie typów produktów, rodzajów usług lub konkretnych procesów ICT pochodzących od dostawcy uwzględnionych w postępowaniu
- **Obowiązek wycofania będzie dotyczył tylko typów sprzętu i oprogramowania wskazanych w decyzji**, a nie wszystkich produktów danego dostawcy
- Podlega natychmiastowemu wykonaniu
- Nie przysługuje ponowne rozpatrzenie sprawy
- Przysługuje na nią skarga do sądu administracynego

Skutki wydania decyzji o uznaniu za DWR

- Zakaz wprowadzania do użytkowania sprzętu lub oprogramowania DWR wskazanych w decyzji
- Obowiązek wycofania z użytkowania sprzętu lub oprogramowania DWR wskazanych w decyzji w określonym terminie
  - Nie później niż **7 lat** od ogłoszenia decyzji w Monitorze Polskim jako ogólna zasada
  - Przedsiębiorcy komunikacji elektronicznej – co do zasady **7 lat**, a **4 lata** od ogłoszenia decyzji na wycofanie w przypadku produktów, procesów i usług określonych w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług
  - Podmioty, do których stosuje się Prawo zamówień publicznych i które nabyły sprzęt lub oprogramowanie określone w decyzji w drodze zamówienia publicznego – co do zasady **7 lat**, a **4 lata** od ogłoszenia decyzji na wycofanie w przypadku produktów, procesów i usług wykorzystywanych do wykonywania funkcji krytycznych określonych w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług

Treść wniosku OW w ramach kontroli po decyzji

- wskazanie podmiotu obowiązanego do przekazania informacji;
- data wydania decyzji o uznaniu za DWR;
- wskazanie zakresu żądanych informacji;
- wskazanie terminu przekazania informacji adekwatnego do zakresu tego żądania, nie krótszego niż 7 dni;
- uzasadnienie;
- pouczenie o zagrożeniu karą pieniężną na gruncie ustawy za niewykonanie obowiązku

Ministerstwo Cyfryzacji

Źr. Schematy przygotowanie i udostępnione przez Ministerstwo Cyfryzacji

Postępowanie o uznanie za DWR nie będzie odnosiło się do wszystkich produktów, usług i procesów ICT, ale tych, które będą wykorzystywane przez podmioty wymienione w ustawie o KSC

Źr. Schematy przygotowanie i udostępnione przez Ministerstwo Cyfryzacji