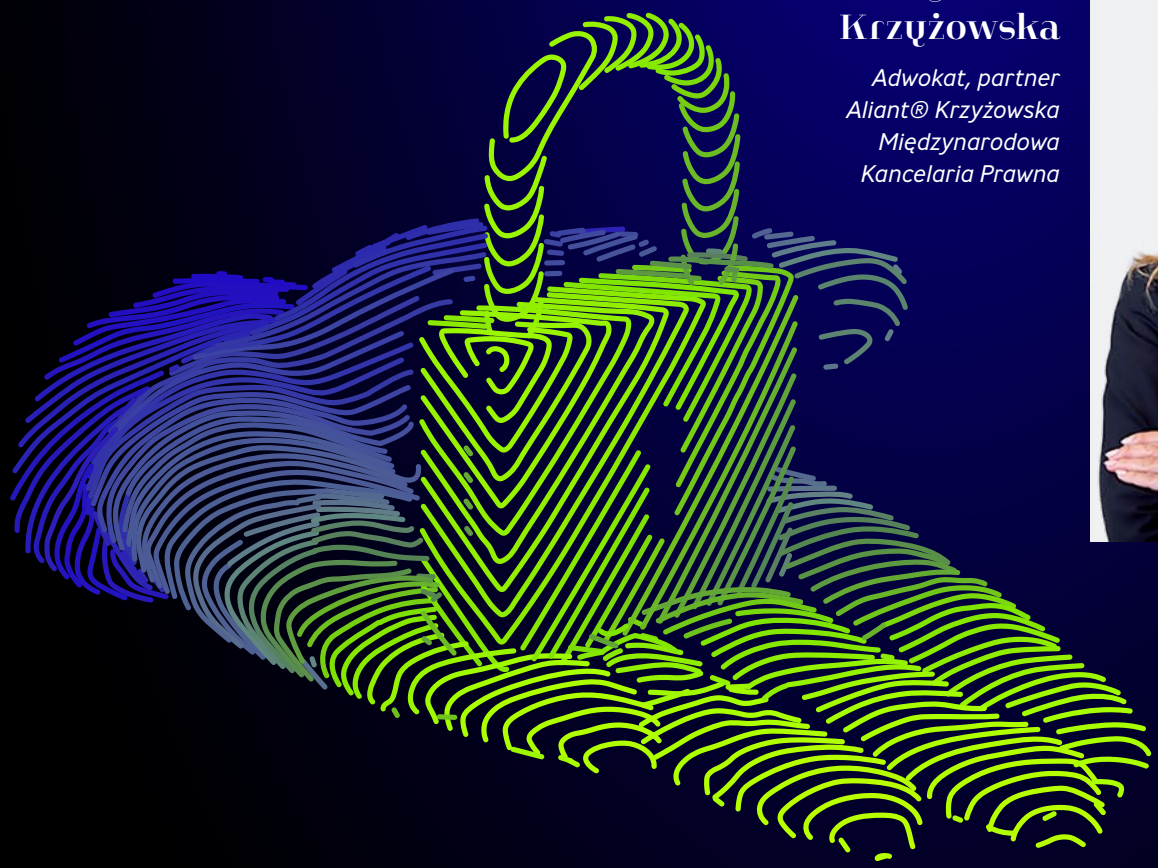
Czy jesteś cyber (bezpieczny)?

Obowiązki dla firm wynikające z dyrektywy NIS 2

Do 17 października 2024 r. państwa członkowskie UE muszą przyjąć i opublikować regulacje niezbędne do zapewnienia zgodności z dyrektywą NIS 2 o cyberbezpieczeństwie, ponieważ obecnie istnieją rozbieżności w wymaganiach dotyczących odporności na cyberzagrożenia w różnych krajach członkowskich. Co to oznacza dla przedsiębiorstw?

Małgorzata Krzyżowska

Adwokat, partner Aliant® Krzyżowska Międzynarodowa Kancelaria Prawna



Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w Unii, zmiany rozporządzenia (UE) nr 910/2014 i dyrektywy (UE) 2018/1972 oraz uchylenia dyrektywy (UE) 2016/1148 (dyrektywa NIS 2) będzie miała zastosowanie do podmiotów publicznych oraz prywatnych, które świadczą usługi lub prowadzą działalność w UE i jednocześnie kwalifikują się jako średnie przedsiębiorstwa lub przekraczają pułapy dla średnich przedsiębiorstw. Przypomnieć tu należy, że zgodnie z przepisami UE pułapy przedstawiają się następująco:

1. Na kategorię przedsiębiorstw mikro, małych i średnich (MŚP) składają się przedsiębiorstwa, które zatrudniają mniej niż 250 osób i których obroty roczne nie przekraczają 50 mln euro, i/lub których roczna suma bilansowa nie przekracza 43 mln euro.
2. W kategorii MŚP małe przedsiębiorstwo jest zdefiniowane jako przedsiębiorstwo zatrudniające mniej niż 50 osób i którego obroty roczne i/lub roczna suma bilansowa nie przekracza 10 mln euro.
3. W kategorii MŚP, przedsiębiorstwo mikro jest zdefiniowane jako przedsiębiorstwo zatrudniające mniej niż 10 osób, i którego obroty roczne i/lub roczna suma bilansowa nie przekracza 2 mln euro. Są to przedsiębiorstwa obejmujące swoim zakresem działalności „sektory kluczowe", takie jak:

- energetyka,
- transport,
- bankowość,
- infrastruktura rynków finansowych,
- opieka zdrowotna,
- sektor wody pitnej,
- ścieki,
- infrastruktura cyfrowa,
- zarządzanie usługami ICT,
- administracja publiczna,
- przestrzeń kosmiczna

oraz sektory „ważne":

- usługi pocztowe i kurierskie,
- gospodarowanie odpadami,
- produkcja, przetwarzanie i dystrybucja chemikaliów,
- produkcja, przetwarzanie i dystrybucja żywności,
- produkcja (szeroko pojęta),
- usługi cyfrowe,
- badania naukowe.

OBOWIĄZEK DLA FIRM I DZIAŁÓW HR

Na działy HR spadną kolejne obowiązki związane z dostosowaniem wewnętrznych regulacji do wymogów ustawowych. Ponieważ nie jest jeszcze procedowany projekt ustawy, aby firmy odpowiednio wcześnie przygotowały się do zmian, już teraz powinny zwrócić uwagę na nowe obowiązki płynące z wytycznych Dyrektywy. Działy HR będą zobligowane do wdrożenia środków technicznych, operacyjnych i organizacyjnych związanych z zarządzaniem ryzykiem (cyberbezpieczeństwo). W tym samym czasie organy zarządzające średnimi przedsiębiorstwami będą zobowiązane do zatwierdzania oraz monitorowania wprowadzania środków zarządzania ryzykiem w dziedzinie cyberbezpieczeństwa. W przypadku zaniedbania tych obowiązków mogą być pociągnięte do odpowiedzialności.

„Kluczowe" oraz „ważne" podmioty będą także zobowiązane do zgłaszania odpowiedniemu CSIRT (https://csirt.gov.pl) poważnych incydentów zgodnie z terminami określonymi przez ustawę. Dodatkowo instytucje te mogą być obowiązane do informowania użytkowników swoich usług o wystąpieniu incydentu, a w szczególnych przypadkach także o znaczącym zagrożeniu cybernetycznym.

Szczegóły dotyczące tych obowiązków będzie można konkretnie wskazać po implementacji dyrektywy, jednak już teraz warto wiedzieć, że „członkowie organów zarządzających istotnych i ważnych podmiotów będą zobowiązani do odbycia szkolenia z zakresu cyberprzestępczości i reagowania na incydenty komputerowe". Zarządy spółek mają zostać zobligowane do regularnego oferowania podobnych szkoleń swoim pracownikom, aby zdobyli oni wystarczającą wiedzę i umiejętności umożliwiające im identyfikację zagrożeń i ocenę praktyk zarządzania ryzykiem cyberbezpieczeństwa oraz ich wpływu na usługi świadczone przez dany podmiot.

Spółki zobligowane będą do podejmowania odpowiednich środków technicznych, operacyjnych i organizacyjnych (szkolenia, komunikacja wewnętrzna, stworzenie polityki cyberbezpieczeństwa, w tym raportowanie i zgłaszanie incydentów, reagowanie i ochrona danych) w celu zarządzania ryzykiem związanym z bezpieczeństwem sieci i systemów informatycznych, które podmioty te wykorzystują do swojej działalności lub do świadczenia swoich usług, oraz w celu zapobiegania lub minimalizowania wpływu incydentów na odbiorców ich usług i na inne usługi.

Mając na uwadze koszt wdrożenia zabezpieczeń, wskazane środki mają zapewniać poziom bezpieczeństwa sieci i systemów informatycznych odpowiedni do stwarzanego ryzyka. Przy ocenie proporcjonalności tych środków należy odpowiednio uwzględnić stopień narażenia podmiotu na ryzyko, wielkość podmiotu oraz prawdopodobieństwo wystąpienia incydentów i ich dotkliwość, w tym ich skutki społeczne i gospodarcze. Środki te opierają się na „podejściu uwzględniającym wszystkie zagrożenia", które ma na celu ochronę sieci i systemów informatycznych oraz fizycznego środowiska tych systemów przed incydentami (zobacz poniżej).

Warto też zwrócić uwagę, że zgodnie z art. 26 (Jurysdykcja i terytorialność), jeżeli podmiot nie ma siedziby w UE, ale oferuje usługi w UE, wyznacza przedstawiciela w UE. Przedstawiciel musi mieć siedzibę w jednym z tych państw członkowskich, w których oferowane są usługi. Uznaje się, że taki podmiot podlega jurysdykcji państwa członkowskiego, w którym przedstawiciel ma siedzibę. W przypadku braku przedstawiciela każde państwo członkowskie, w którym podmiot świadczy usługi, może podjąć działania prawne przeciwko podmiotowi w związku z naruszeniem dyrektywy.

CO DYREKTYWA MA ZABEZPIECZAĆ?

Celem dyrektywy NIS 2 jest podniesienie poziomu bezpieczeństwa cybernetycznego w Unii Europejskiej. W motywach tej dyrektywy zwraca się uwagę na obecne rozbieżności w wymaganiach dotyczących odporności na cyberzagrożenia w różnych krajach członkowskich, co prowadzi do fragmentaryzacji rynku wewnętrznego. Problem ten wynika z faktu, że państwa członkowskie mają dużą swobodę w zakresie wdrożenia dyrektywy NIS (poprzedniej dyrektywy), co skutkuje różnymi wymaganiami i metodami nadzoru. Dlatego nowa dyrektywa ma na celu wyeliminowanie tych rozbieżności i poprawę cyberbezpieczeństwa w obliczu dynamicznego rozwoju technologii. Chodzi o osiągnięcie wysokiego wspólnego poziomu bezpieczeństwa cybernetycznego w całej UE, aby zwiększyć efektywność rynku wewnętrznego.

Dyrektywa NIS 2 określa obowiązki państw członkowskich, takie jak przyjęcie krajowych strategii cyberbezpieczeństwa i utworzenie odpowiednich organów ds. zarządzania kryzysowego w cyberbezpieczeństwie, punktów kontaktowych ds. cyberbezpieczeństwa i zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT).

Dodatkowo dyrektywa reguluje kwestie zarządzania ryzykiem w cyberbezpieczeństwie oraz obowiązki

Zapewnienie cyberbezpieczeństwa powinno obejmować „co najmniej" następujące elementy:

- polityki dotyczące analizy ryzyka i bezpieczeństwa systemów informatycznych;
- obsługę incydentów;
- ciągłość działania, taką jak zarządzanie kopiami zapasowymi i odzyskiwanie danych po awarii oraz zarządzanie kryzysowe;
- bezpieczeństwo łańcucha dostaw, w tym aspekty związane z bezpieczeństwem dotyczące relacji między każdym podmiotem a jego bezpośrednimi dostawcami lub usługodawcami;
- bezpieczeństwo nabywania, rozwijania i utrzymywania sieci i systemów informatycznych, w tym postępowanie z lukami w zabezpieczeniach i ich ujawnianie;
- polityk i procedur służących ocenie skuteczności środków zarządzania ryzykiem w zakresie cyberbezpieczeństwa;
- podstawowe praktyki higieny cybernetycznej i szkolenia w zakresie cyberbezpieczeństwa;
- polityki i procedury dotyczące stosowania kryptografii oraz, w stosownych przypadkach, szyfrowania;
- bezpieczeństwo zasobów ludzkich, zasady kontroli dostępu i zarządzanie aktywami;
- w stosownych przypadkach korzystanie z uwierzytelniania wieloskładnikowego lub rozwiązań uwierzytelniania ciągłego, zabezpieczonej komunikacji głosowej, wideo i tekstowej oraz zabezpieczonych systemów komunikacji awaryjnej w ramach podmiotu.

Członkowie organów zarządzających istotnych i ważnych podmiotów będą zobowiązani do odbycia szkolenia z zakresu cybeprzestępczości i reagowania na incydenty komputerowe.

związane ze zgłaszaniem incydentów, nakładając je na określone podmioty. Dyrektywa NIS 2 obejmuje także zasady i obowiązki dotyczące wymiany informacji o cyberbezpieczeństwie oraz nadzoru i egzekwowania przepisów, które spoczywają na państwach członkowskich.

KONTROLA I EGZEKWOWANIE PRZEPISÓW

Istotną kwestią jest szeroki zakres uprawnień, który otrzymają organy nadzorcze w dziedzinie nadzoru i egzekwowania przepisów. Będą one obejmować szeroki zakres działań, jednak szczegółowa lista tych uprawnień będzie zależała od tego, czy dotyczą one podmiotów z sektora „kluczowego" czy „ważnego".

Do działań, które będą stosowane zarówno w przypadku podmiotów kluczowych, jak i ważnych, można zaliczyć:
Przeprowadzanie niezależnych i ukierunkowanych audytów bezpieczeństwa.
• Wnioskowanie o udostępnienie informacji, dostępu do danych i dokumentów.
• Wydawanie nakazów w celu zapewnienia zgodności z przepisami dyrektywy NIS 2 lub zaprzestania określonej działalności.
• Nakazanie wdrożenia zaleceń wynikających z audytu bezpieczeństwa.
• W przypadku podmiotów z sektora „kluczowego" istnieje również możliwość podjęcia działań, takich jak tymczasowe zawieszenie certyfikacji lub zezwolenia na świadczenie usług lub prowadzenie działalności przez dany podmiot, jeśli powyższe środki okazują się nieskuteczne. Ponadto można nałożyć tymczasowy zakaz pełnienia funkcji zarządczych w takim podmiocie.

Warto też zwrócić uwagę, że przedsiębiorstwa, które nie zastosują wymogów nałożonych przez ustawę, ryzykują tymczasowym zawieszeniem certyfikacji lub zezwolenia na świadczenie części lub całości usług danego podmiotu. Organy mają być też uprawnione do orzeczenia tymczasowego zakazu sprawowania funkcji zarządczych przez osobę fizyczną wykonującą obowiązki zarządcze (zarząd, dyrektor generalny, wspólnicy spółek osobowych).

Z uwagi na dotkliwość takich kar i ich wpływ na działalność podmiotów, a ostatecznie na użytkowników, takie tymczasowe zawieszenia lub zakazy mają być stosowane odpowiednio do wagi naruszenia i z uwzględnieniem okoliczności danej sprawy, w tym tego, czy naruszenie było umyślne, czy też wynikało z niedbalstwa (np. brak wprowadzenia procedur, zaleceń i ignorowanie tych obowiązków), oraz działań podjętych, aby zapobiec szkodom majątkowym lub niemajątkowym lub je ograniczyć. Takie tymczasowe zawieszenia lub zakazy mają być stosowane w ostateczności, tj. po wyczerpaniu innych stosownych środków egzekwowania przepisów (zostaną one określone w ustawie). Środki te będą stosowane dopóki podmioty, których to dotyczy, nie podejmą niezbędnych działań w celu usunięcia nieprawidłowości lub nie spełnią wymagań właściwego organu, z których tytułu zastosowano takie tymczasowe zawieszenia lub zakazy.

Należy też pamiętać, że równolegle w mocy pozostaje Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554, które należy uznać za sektorowy akt prawny Unii powiązany z ww. dyrektywą w odniesieniu do podmiotów finansowych. Zamiast przepisów omawianej wyżej dyrektywy zastosowanie powinny mieć przepisy rozporządzenia (UE) 2022/2554 dotyczące zarządzania ryzykiem związanym z technologiami informacyjno-komunikacyjnymi (ICT), zarządzania incydentami związanymi z ICT, a w szczególności zgłaszania poważnych incydentów związanych z ICT, a także testowania operacyjnej odporności cyfrowej, mechanizmów wymiany informacji oraz ryzyka związanego z zewnętrznymi dostawcami ICT.

Do podmiotów finansowych objętych rozporządzeniem (UE) 2022/2554 nie będą miały zatem zastosowania przepisy nowo wprowadzanej dyrektywy dotyczące zarządzania ryzykiem w cyberbezpieczeństwie i obowiązki w zakresie zgłaszania incydentów oraz nadzoru i egzekwowania prawa. ● ©