Komentarz do ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa

(Dz.U. z 2018 r. poz. 1560)

Rozdział 1. Przepisy ogólne

Art. 1. [Zakres przedmiotowy ustawy i wyłączenia podmiotowe]

1. Ustawa określa:

1) organizację krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu;

2) sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy;

3) zakres Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej.

2. Ustawy nie stosuje się do:

1) przedsiębiorców telekomunikacyjnych, o których mowa w ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. z 2017 r. poz. 1907 i 2201 oraz z 2018 r. poz. 106, 138, 650 i 1118), w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów;

2) dostawców usług zaufania, którzy podlegają wymogom art. 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz.Urz. UE L 257 z 28.08.2014, str. 73);

3) podmiotów wykonujących działalność leczniczą, tworzonych przez Szefa Agencji Bezpieczeństwa Wewnętrznego lub Szefa Agencji Wywiadu.

Powiązania z innymi przepisami:

- art. 175 i n. PrTelekom,
- art. 6 w zw. z art. 37 ust. 5–5a DziałLeczU,
- art. 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) Nr 910/2014 z 23.7.2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz.Urz. UE L 2014 Nr 257, s. 73).

I. Implementacja dyrektywy NIS

1. Ustawa o krajowym systemie cyberbezpieczeństwa stanowi przede wszystkim implementację dyrektywy NIS. W niektórych miejscach zakres regulacji CyberbezpU jest szerszy. Dotyczy to sytuacji, dla których dyrektywa NIS przewidywała minimalny poziom harmonizacji, dopuszczając wprowadzenie przez Państwa członkowskie dalej idących przepisów, a konieczne było zastosowanie rozwiązania specyficznego dla Polski. Dyrektywa NIS wprowadziła wspólne definicje, zaplecze instytucjonalne oraz podstawowe obowiązki dla wszystkich krajów członkowskich w zakresie cyberbezpieczeństwa.

2. Dyrektywa NIS wynikała ze Strategii Cyberbezpieczeństwa Unii Europejskiej [Wysoki Przedstawiciel Unii Europejskiej do spraw Zagranicznych i Polityki Bezpieczeństwa oraz Komisja Europejska, Wspólny Komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń, JOIN(2013) 1 final], opublikowanej 7.2.2013 r. Dyrektywa NIS była wskazana jako środek realizacji jednego z pięciu głównych priorytetów – osiągnięcia odporności na zagrożenie cybernetyczne. Po blisko trzyletnim procesie legislacyjnym, dyrektywa NIS została przyjęta przez Radę Unii Europejskiej i Parlament w dniu 6.7.2016 r. Nowe elementy wprowadzone przez nią do europejskiego porządku prawnego to:

1) stworzenie wspólnej siatki pojęciowej (incydent, sieci i systemy, postępowanie w razie incydentu),
2) ustanowienie zespołów CSIRT, organów właściwych oraz pojedynczego punktu kontaktowego w każdym państwie członkowskim,
3) wyodrębnienie operatorów usług kluczowych w wybranych sektorach gospodarki i nałożenie na nich nowych obowiązków,
4) wyróżnienie dostawców usług cyfrowych i nałożenie na nich nowych, ale łagodniejszych niż u operatorów, obowiązków,
5) nałożenie na państwa obowiązku przygotowania krajowej strategii w zakresie bezpieczeństwa sieci i systemów informatycznych,
6) zasady współpracy pomiędzy państwami członkowskimi (Sieć CSIRT i Grupa Współpracy).

3. Dyrektywa NIS nakłada minimalne wymogi na zespoły CSIRT, określa podstawowe zasady identyfikacji operatorów usług kluczowych, określa minimalne wymogi bezpieczeństwa i progi zgłaszania incydentów dla dostawców usług cyfrowych oraz nakłania do promowania normalizacji (zgodnie z zasadą neutralności technologicznej) i dobrowolnego zgłaszania incydentów.

4. Ustawa o krajowym systemie cyberbezpieczeństwa została wpisana do wykazu prac legislacyjnych Rady Ministrów (pod numerem UD31) jeszcze przed wejściem w życie dyrektywy NIS. Na przedłużenie prac nad implementacją wpłynęły m.in. długi czas prac wewnątrz rządu oraz proces pre- i konsultacji (wszystkie dokumenty dotyczące projektu ustawy są dostępne na stronie Rządowego Centrum Legislacji: https://legislacja.rcl.gov.pl/projekt/12304650, dostęp: 26.4.2019 r.). Mniej więcej w tym samym okresie prowadzone były prace nad Strategią Cyberbezpieczeństwa RP, które zostały przyjęte

przez Radę Ministrów w listopadzie 2017 r. (uchwała Nr 52/2017 Rady Ministrów z 27.4.2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022). Ustawa o krajowym systemie cyberbezpieczeństwa została przyjęta przez Sejm dwa miesiące po wyznaczonym przez Komisję terminie, kiedy około połowa krajów Unii nie dokonała jeszcze implementacji.

5. Ustawa o krajowym systemie cyberbezpieczeństwa wykracza poza implementację minimalną – **zakres ustawy został rozszerzony o wybrane elementy bezpieczeństwa narodowego (współpraca zespołów CSIRT, incydenty krytyczne) i instytucjonalne (utworzenie funkcji Pełnomocnika Rządu do spraw Cyberbezpieczeństwa oraz Kolegium do spraw Cyberbezpieczeństwa). Rozszerzono również zakres przedmiotowy, obejmując więcej sektorów gospodarki w stosunku do dyrektywy NIS** (zob. komentarz do art. 5 CyberbezpU).

6. Doprecyzowano też ogólne przepisy z dyrektywy NIS, tworząc model uwzględniający polską specyfikę w ramach unijnego prawa. Wybrano tryb wyznaczania operatorów usług kluczowych w drodze decyzji administracyjnej – wykaz operatorów prowadzi minister właściwy do spraw informatyzacji. Wskazano szczegółowo obowiązki operatorów. Dostawcy usług cyfrowych nie są w żaden sposób wyznaczani, muszą dokonać analizy przepisów ustawy i autoidentyfikacji. Wydzielono trzy zespoły CSIRT oraz podzielono odpowiedzialność organów właściwych do spraw cyberbezpieczeństwa według sektorów gospodarki i działów administracji rządowej – rozdzielono w ten sposób część techniczną systemu od części administracyjnej. Podzielono zadanie ochrony cyberprzestrzeni RP na część cywilną i wojskową.

II. Zakres obowiązywania ustawy

7. Ustawa o krajowym systemie cyberbezpieczeństwa określa organizację krajowego systemu cyberbezpieczeństwa (por. art. 4). Każda grupa podmiotów (operatorzy usług kluczowych, dostawcy usług cyfrowych, podmioty publiczne, CSIRT, organy właściwe, Pojedynczy Punkt Kontaktowy, wybrani ministrowie) ma określone zadania, uprawnienia i obowiązki związane z zapewnieniem cyberbezpieczeństwa.

8. Ponadto CyberbezpU określa sposób nadzoru i kontroli przez organy właściwe nad wybranymi uczestnikami systemu (por. rozdział 11 CyberbezpU).

Ważne

Ustawa określa zakres Strategii Cyberbezpieczeństwa RP, która zastąpi najpóźniej do końca października 2019 r. obecny dokument strategiczny, tzn. Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022, przyjęte uchwałą Rady Ministrów w 2017 r.

III. Wyłączenia ustawowe

9. Niezwykle istotne są wyłączenia spod zakresu CyberbezpU. Ustawa nie obejmuje trzech grup podmiotów. Dwa pierwsze przypadki wynikają wprost z implementacji dyrektywy

NIS, trzeci to wyłączenie wynikające z konieczności zapewnienia bezpieczeństwa narodowego.

Zgodnie z dyrektywą NIS nie stosuje się jej wymogów dotyczących bezpieczeństwa i zgłaszania incydentów do przedsiębiorców, którzy podlegają wymogom art. 13a i 13b dyrektywy 2002/21/WE Parlamentu Europejskiego i Rady z 7.3.2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (dyrektywa ramowa) (Dz.Urz. WE L 2002 Nr 108, s. 33), transponowanej do polskiego prawa przez PrTelekom w art. 175 i n., ani do dostawców usług zaufania, którzy podlegają wymogom określonym w art. 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) Nr 910/2014 z 23.7.2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (rozporządzenie eIDAS) (Dz.Urz. UE L 2014 Nr 257, s. 73).

10. O ile przypadek dostawców usług zaufania nie wymaga specjalnego komentarza – są to zazwyczaj wyspecjalizowane firmy o wąskim zakresie działania – o tyle przypadek przedsiębiorców telekomunikacyjnych już tak. Zgodnie z motywami dyrektywy NIS przedsiębiorcy telekomunikacji na mocy dyrektywy 2002/21/WE podlegają już szczególnym wymogom bezpieczeństwa w zakresie udostępniania publicznych sieci łączności i świadczenia publicznie dostępnej usługi łączności elektronicznej w rozumieniu PrTelekom. Wyłączenie dotyczy jednak tylko tych usług.

11. Dyrektywa NIS zabrania zatem nie tyle nakładania w ogóle nowych obowiązków na przedsiębiorców telekomunikacyjnych, ile nakładania nowych obowiązków w ramach usług określonych w PrTelekom.

Przykład

Jeśli przedsiębiorca świadczy usługi kluczowe jako dostawca usług DNS w sektorze infrastruktury cyfrowej i został uznany za operatora usługi kluczowej to wymogi bezpieczeństwa i zgłaszania incydentów dotyczą tylko tych usług DNS, a nie całej działalności telekomunikacyjnej.

12. Ostatnie wyłączenie dotyczy zakładów leczniczych utworzonych przez Agencję Bezpieczeństwa Wewnętrznego lub Agencję Wywiadu. Są to specjalne placówki, podlegające wyłączeniom na mocy DziałLeczU – nie podlegają przepisom o samodzielnych publicznych zakładach opieki zdrowotnej, mają ograniczone grono odbiorców i odrębne zasady przeprowadzania w nich kontroli. Ze względu na specyfikę działalności uznano za uzasadnione wyłączyć te podmioty spod CyberbezpU.

Art. 2. [Słowniczek]

Użyte w ustawie określenia oznaczają:

1) **CSIRT GOV – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego;**

2) **CSIRT MON – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Ministra Obrony Narodowej;**
3) **CSIRT NASK – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy;**
4) **cyberbezpieczeństwo – odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;**
5) **incydent – zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo;**
6) **incydent krytyczny – incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV;**
7) **incydent poważny – incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej;**
8) **incydent istotny – incydent, który ma istotny wpływ na świadczenie usługi cyfrowej w rozumieniu art. 4 rozporządzenia wykonawczego Komisji (UE) 2018/151 z dnia 30 stycznia 2018 r. ustanawiającego zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ (Dz.Urz. UE L 26 z 31.01.2018, str. 48), zwanego dalej „rozporządzeniem wykonawczym 2018/151";**
9) **incydent w podmiocie publicznym – incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny, o którym mowa w art. 4 pkt 7–15;**
10) **obsługa incydentu – czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu;**
11) **podatność – właściwość systemu informacyjnego, która może być wykorzystana przez zagrożenie cyberbezpieczeństwa;**
12) **ryzyko – kombinację prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji;**
13) **szacowanie ryzyka – całościowy proces identyfikacji, analizy i oceny ryzyka;**
14) **system informacyjny – system teleinformatyczny, o którym mowa w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2017 r. poz. 570 oraz z 2018 r. poz. 1000 i 1544), wraz z przetwarzanymi w nim danymi w postaci elektronicznej;**

15) usługa cyfrowa – usługę świadczoną drogą elektroniczną w rozumieniu przepisów ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2017 r. poz. 1219 oraz z 2018 r. poz. 650), wymienioną w załączniku nr 2 do ustawy;
16) usługa kluczowa – usługę, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymienioną w wykazie usług kluczowych;
17) zagrożenie cyberbezpieczeństwa – potencjalną przyczynę wystąpienia incydentu;
18) zarządzanie incydentem – obsługę incydentu, wyszukiwanie powiązań między incydentami, usuwanie przyczyn ich wystąpienia oraz opracowywanie wniosków wynikających z obsługi incydentu;
19) zarządzanie ryzykiem – skoordynowane działania w zakresie zarządzania cyberbezpieczeństwem w odniesieniu do oszacowanego ryzyka.

Powiązania z innymi przepisami:

- art. 8, 11–13, 18–19, 22–23, 26–27 CyberbezpU.

I. Uwagi ogólne

1. Definicje w CyberbezpU dzielą się na te wynikające wprost z dyrektywy NIS (pkt 4, 7, 8, 10, 12 i 14–16) oraz te, które zostały dodane, aby dostosować nowy system cyberbezpieczeństwa do polskich warunków (pkt 1–3, 5, 6, 9, 11, 13 i 17–19). Definicje musiały być zgodne z dyrektywą NIS, która ich wymagała, jednak odpowiednio dostosowane do warunków polskiej legislacji.

II. Cyberbezpieczeństwo

2. Definicja cyberbezpieczeństwa w CyberbezpU to dostosowana do polskich warunków definicja bezpieczeństwa sieci i systemów z art. 4 pkt 2 dyrektywy NIS. Zgodnie z tą definicją bezpieczeństwo sieci i systemów informatycznych oznacza odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przechowywanych lub przekazywanych, lub przetwarzanych danych lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy informatyczne.

Transpozycja przepisów wprost nie jest zwyczajowym rozwiązaniem w polskiej legislacji – priorytet ma spójność krajowego systemu prawa. Dlatego definicję skrócono o elementy, które w rozumieniu polskiej legislacji nie mają znaczenia. Jednym z nich jest wskazanie na „dany poziom zaufania", które jest istotne w kontekście technicznym, ale nie legislacyjnym. Podobnie odstąpiono od rozróżnienia na usługi „dostępne" i „oferowane".

Definicja wskazuje na **cztery elementy bezpieczeństwa danych – poufność, autentyczność, integralność i dostępność. Są to również atrybuty bezpieczeństwa informacji.**

Zgodnie z normą PN-EN ISO/IEC 27000 „bezpieczeństwo informacji" to zapewnienie poufności, integralności i dostępności informacji – z możliwością rozszerzenia ochrony o inne atrybuty: autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Każdy z atrybutów został starannie zdefiniowany na potrzeby zarządzania informacji.

Poufność oznacza, że informacja nie jest ujawniana ani udostępniana nieuprawnionym podmiotom. **Integralność** – że informacja jest poprawna i kompletna; wreszcie **dostępność** – że informacja jest dostępna na żądanie uprawnionej osoby. Praktycznie każda informacja ma te trzy atrybuty, stąd nazywane są one razem triadą bezpieczeństwa informacji albo CIA (od angielskich terminów: *confidentiality*, *integrity*, *availability*). Pozostałe atrybuty są opcjonalne i nie występują zawsze.

Przykład

Niezaprzeczalność, czyli możliwość udowodnienia, że dane wydarzenie miało miejsce, jest niezwykle istotna dla podpisów cyfrowych oznaczanych znacznikami czasu.

Definicja w dyrektywie NIS rozszerzyła podstawowe trzy atrybuty o czwarty – **autentyczność**, czyli właściwość, która polega na tym, że podmiot jest tym, za kogo się podaje.

Jeśli chodzi o **odporność**, to zgodnie z definicją słownikową: „odporny – niewrażliwy na wpływy fizyczne lub moralne" (Słownik języka polskiego PWN, https://sjp.pwn.pl/szukaj/odporność.html, dostęp: 2.5.2019 r.), także „odporność – (…) zdolność przeciwstawiania się czemuś, niepoddawania się jakiemuś działaniu, naciskowi, wpływowi itp., niewrażliwość na co; wytrzymałość" [*W. Doroszewski* (red.), Słownik języka polskiego, http://www.sjpd.pwn.pl/haslo/odporność/, dostęp: 2.5.2019 r.]. Angielska wersja dyrektywy NIS używa terminu „*ability to resist (…) any action*". Według Oxford Learner's Dictionary „*resistance*" to m.in. „*the power not to be affected by something*". Niemiecka wersja bardziej bezpośrednio wskazuje: „*die Fähigkeit (…) alle Angriffe abzuwehren*", gdzie „*Angriff*" oznacza także „atak", a „*zu abwehren*" oznacza przede wszystkim „bronić".

Polska zarówno w tłumaczeniu, jak i transpozycji skupiła się na „odporności" jako kluczowym elemencie definicji cyberbezpieczeństwa. O ile bezpieczeństwo (zarówno w pojęciu „*safety*", jak i „*security*") odnosi się do stanu lub procesu związanego z poczuciem bezpieczeństwa albo poziomem zabezpieczeń, o tyle odporność (także „cyberodporność" – „*cyber resilience*") odnosi się do zdolności ciągłego dostarczania zamierzonego wyniku bez względu na przeciwności. Tak to przedstawili np. *F. Bjorck* i in., Cyber Resilience – fundamentals for a definition, Advances in Intelligent Systems and Computing, styczeń 2015; w kontekście NATO przedstawia się odporność jako „zdolność do odbicia się od cyberataku i utrzymanie zdolności operacyjnej" (*L. Pijnenburg Muller*, *T. Stevens*, Upholding the NATO cyber pledge. Cyber Deterrence and Resilience: Dilemmas in NATO defence and security politics, Policy Brief 2017, Nr 5, Norwegian Institute of International Afairs). Cyberodporność to także jeden z filarów Strategii Cyberbezpieczeństwa Unii

Europejskiej (Wspólny Komunikat do Parlamentu Europejskiego i Rady, Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego Unii Europejskiej, JOIN/2017/0450 final).

Problematyczna w tym miejscu okazuje się definicja w projekcie unijnego rozporządzenia Akt o Cyberbezpieczeństwie [Proposal for a Regulation of the European Parliament and of the Council on ENISA, the „EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification („Cybersecurity Act"), COM/2017/0477 final – 2017/0225 (COD)]. Zgodnie z projektem, który jest już na bardzo zaawansowanym etapie legislacyjnym, przyjmuje się definicję cyberbezpieczeństwa na poziomie unijnym. Różni się ona od przyjętej w dyrektywie NIS definicji wskazującej na odporność. Zgodnie z nią, cyberbezpieczeństwo to wszystkie czynności niezbędne, aby chronić sieci i systemy informacyjne, ich użytkowników oraz inne osoby przed cyberzagrożeniami (tłum. własne; w wersji angielskiej: *„cybersecurity" comprises all activities necessary to protect network and information systems, their users, and affected persons from cyber threats*). Jest to definicja ogólniejsza niż dotychczasowa i **istnieje ryzyko konfliktu pomiędzy cyberbezpieczeństwem z rozporządzenia a cyberbezpieczeństwem z CyberbezpU.**

III. System teleinformatyczny a system informacyjny

3. W polskim prawie doszło do kilku prób zdefiniowania pojęcia systemu teleinformatycznego. Powstawały one w różnych kontekstach i różnym czasie.

4. Pierwsza istotna dla niniejszego opracowania definicja została wprowadzona przez SwiadUsłElektU. Definicję tę powtórzyła późniejsza InformPodPublU. W 2008 r., w wyniku ustawy z 4.9.2008 r. o zmianie ustaw w celu ujednolicenia terminologii informatycznej (Dz.U. Nr 171, poz. 1056), definicja została wprowadzona do wielu obowiązujących wówczas aktów prawnych. Warto jednak wskazać, że w DziałAntyterrU – mimo iż wyraźnie wynika z kontekstu regulacji, że ustawodawca ma na myśli system teleinformatyczny w rozumieniu ww. definicji, używa sformułowania „systemy informatyczne i teleinformatyczne", podczas gdy BezpWewnU posługuje się terminem „systemy teleinformatyczne organów administracji publicznej lub system sieci teleinformatycznych" (por. np. art. 32a BezpWewnU).

5. Nieco inne podejście przyjął MON, który w swoich wewnętrznych regulacjach zdefiniował system teleinformatyczny jako system, który tworzą urządzenia, narzędzia, metody postępowania i procedury stosowane przez wyspecjalizowanych pracowników, w sposób zapewniający wytwarzanie, przechowywanie, przetwarzanie lub przekazywanie informacji [tak decyzja MON Nr 357/MON z 29.7.2008 r. w sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej (Dz.Urz. MON Nr 16, poz. 205)].

6. Ustawa z 26.4.2007 r. o zarządzaniu kryzysowym (t.j. Dz.U. z 2018 r. poz. 1401) wskazuje z kolei na „sieci teleinformatyczne", bez wskazywania wprost urządzeń końcowych. Z powyższych rozważań wyraźnie wynika, że mimo starań, zawsze część pojęć wymknie się próbom ujednolicania definicji.

7. Dyrektywa NIS przyjęła nową definicję dla **systemów i sieci teleinformatycznych**, obejmującą:

1) sieci łączności elektronicznej w rozumieniu dyrektywy 2002/21/WE,
2) wszelkie urządzenia lub grupy wzajemnie połączonych lub powiązanych urządzeń, z których jedno lub większa ich liczba, wykonując program, dokonuje automatycznego przetwarzania danych cyfrowych lub
3) dane cyfrowe przechowywane, przetwarzane, odzyskiwane lub przekazywane w celu ich eksploatacji, użycia, ochrony i utrzymania.

8. Istniejąca w ŚwiadUsłElektU definicja systemu teleinformatycznego zawierała pierwszy i drugi element definicji, nie objęła jednak danych cyfrowych. W tym celu należało opracować definicję obejmującą również dane cyfrowe (por. art. 2 pkt 14 CyberbezpU).

IV. Incydent, rodzaje incydentów

9. Dyrektywa NIS używa w słowniczku jednej definicji dotyczącej „incydentu", później rozróżniając, że incydenty mogą dotyczyć różnego stopnia zagrożenia i różnych podmiotów. Dla czytelności obowiązków, wybrano model definicyjny, w którym wskazano różne rodzaje incydentów wprost w słowniczku. W ten sposób pojawiły się następujące definicje:

1) incydent,
2) incydent poważny,
3) incydent istotny,
4) incydent w podmiocie publicznym,
5) incydent krytyczny.

10. Incydent (art. 2 pkt 5 CyberbezpU – zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo) jest tzw. incydentem „zwykłym", niepodlegającym obowiązkowi zgłaszania. Może on dotyczyć każdego podmiotu (także spoza krajowego systemu cyberbezpieczeństwa) i nie ma określonych progów ani wartości. Jest to najogólniejsza i najbardziej pojemna definicja, która może być potencjalnie stosowana także przez inne akty prawne, bo nie odnosi się do żadnych elementów sektorowych. Ustawa o krajowym systemie cyberbezpieczeństwa dodała w art. 81 nowy ust. 1a w art. 175a PrTelekom, odnoszący się właśnie do naruszenia bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych, które miało istotny wpływ na funkcjonowanie sieci lub usług, które mogą być jednocześnie incydentami w rozumieniu CyberbezpU. **Incydent ma charakter potencjalny – samo zdarzenie, które mogło mieć niekorzystny wpływ, ale zostało odparte lub powstrzymane, też jest incydentem bezpieczeństwa.** Przykładem może tu być znaleziony na parkingu zainfekowany nośnik typu pendrive czy też odparty atak DDoS. Incydent „zwykły" to najszersza kategoria zdarzeń, dlatego nie podlega obowiązkowemu zgłaszaniu. Może jednak być przekazywany jako dobrowolne zgłoszenie (por. komentarz do art. 13).

11. Incydent poważny (art. 2 pkt 7 CyberbezpU – incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej) podlega obowiązkowi zgłaszania przez operatorów usług kluczowych.

Ważne

O tym co jest, a co nie jest incydentem poważnym, mowa jest w rozporządzeniu Rady Ministrów z 31.10.2018 r. w sprawie progów uznania incydentu za poważny (Dz.U. z 2018 r. poz. 2180). Incydenty poważne dotyczą tylko usług kluczowych. Rozporządzenie wskazuje sektor, podsektor, nazwę zdarzenia oraz progi istotności, które muszą być przekroczone, aby incydent można było uznać za poważny. Brak dokonania zgłoszenia incydentu poważnego grozi nałożeniem administracyjnej kary finansowej.

12. Incydent istotny [art. 2 pkt 8 CyberbezpU – incydent, który ma istotny wpływ na świadczenie usługi cyfrowej w rozumieniu art. 4 rozporządzenia wykonawczego Komisji (UE) 2018/151 z 30.1.2018 r. ustanawiające zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ (Dz.Urz. UE L 2018 Nr 26, s. 48)] jest to incydent podlegający obowiązkowi zgłaszania przez dostawców usług cyfrowych. Progi incydentu istotnego są określone w rozporządzeniu wykonawczym 2018/151. Więcej o progach incydentu istotnego w komentarzu do art. 17.

13. Incydent w podmiocie publicznym (art. 2 pkt 9 CyberbezpU – incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny, o którym mowa w art. 4 pkt 7–15) to incydent podlegający obowiązkowi zgłaszania przez podmioty publiczne. Komentowana ustawa (ani żadna inna ustawa) nie definiuje wprost, czym są zadania publiczne. Konieczne jest tutaj sięgnięcie do interpretacji z innych dziedzin.

14. W nauce prawa administracyjnego oraz w orzecznictwie podejmowane są próby doprecyzowania, czym są zadania publiczne. Pojęcie to łączy się z pojęciem administracji publicznej i wskazuje się, że „za zadania publiczne uznać zadania administracji, które mają być wykonane w celu realizacji potrzeb powszechnych, których zaspokojenie jest obowiązkiem administracji regulowanym przepisami prawa" (*D. Kurzyna-Chmiel*, Oświata jako zadanie publiczne, Warszawa 2013, s. 112–118), a także przejęte przez państwo zaspokajanie zbiorowych i indywidulanych potrzeb człowieka, wynikających ze współżycia ludzi w społeczeństwie [*S. Fundowicz*, Dynamiczne rozumienie zadania publicznego, (w:) Między tradycją a przyszłością w nauce prawa administracyjnego. Księga jubileuszowa dedykowana Profesorowi Janowi Bociowi, red. *J. Supernat*, Wrocław 2009, s. 155]. Zakres tego pojęcia podlega ciągłym zmianom, bo zmianom ulega także rola administracji – od roli „nocnego stróża" po aktywnego uczestnika życia społecznego. Jednak zawsze zadania publiczne wiążą się z chronionym przez nie dobrem wspólnym i realizacją interesu publicznego. Można zatem uznać, że treścią zadań publicznych, w interesującym nas kontekście, jest przede wszystkim dostarczanie określonych usług o charakterze społecznym na rzecz zbiorowości (*D. Kurzyna-Chmiel*, Oświata…, s. 112–118).

15. Incydent krytyczny (art. 2 pkt 6 CyberbezpU – incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów

gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV), jest jedynym incydentem, który nie podlega klasyfikacji przez podmiot, którego dotyczy. Jest to specjalna klasa incydentów wynikająca z potrzeby specjalnego traktowania przez CSIRT incydentów, które stanowią zagrożenie dla bezpieczeństwa narodowego.

Ważne

Incydentem krytycznym może być każdy incydent – decyzja o klasyfikacji zależy od właściwego zespołu CSIRT. Operatorzy usług kluczowych nie muszą się zajmować klasyfikacją incydentu krytycznego – nie mają takiego obowiązku. Może się jednak zdarzyć, że incydent, który dla danej organizacji jest incydentem zwykłym, w skali kraju – np. ze względu na zasięg geograficzny – jest incydentem krytycznym.

16. Definicje incydentu w podmiocie publicznym i incydentu krytycznego nie wynikają z dyrektywy NIS, ale były konieczne dla uzupełnienia systemu zgłaszania incydentów.

V. Obsługa incydentu, zarządzanie incydentem

17. Definicja obsługi incydentu (art. 2 pkt 10 CyberbezpU) to dostosowana definicja „postępowania z incydentem" (ang. *incident handling*) z dyrektywy NIS. Komentowana ustawa odniosła się tutaj do terminologii znanej z ITIL (*Information Technology Infrastructure Library*, ustandaryzowane podejście i zbiór dobrych praktyk stosowanych w zarządzaniu usługami IT), która przyjęła następujące elementy procesu: identyfikacja, rejestracja, nadawanie priorytetów, wstępna diagnoza, eskalacja, śledztwo i diagnoza, rozwiązanie i przywrócenie usługi, zamknięcie incydentu. Ustawa o krajowym systemie cyberbezpieczeństwa odeszła od podejścia ściśle usługowego, wskazując na następujące czynności operacyjne i techniczne, będące etapami obsługi incydentu:

1) wykrywanie – punkt startowy procesu obsługi; każdy incydent ma zostać wykryty, konieczna jest tu aktywność operatora – zaniechanie działalności na rzecz tego etapu będzie oznaczać brak realizacji obowiązku ustawowego;
2) rejestrowanie – niezbędne jest prowadzenie rejestru incydentów, które miały miejsce w danym systemie;
3) analizowanie – operator musi dokonać (wstępnej) analizy incydentu;
4) klasyfikowanie – konieczne jest dokonanie klasyfikacji incydentu; ustawa nie wskazuje przyjętego modelu klasyfikacji, ale przyjęcie tego samego modelu co zespół CSIRT wspierający obsługę przyspieszy uzyskanie wsparcia;
5) priorytetyzacja – oprócz skategoryzowania incydentu operator musi być w stanie określić jego priorytet – czy jest to incydent do obsługi w pierwszej kolejności, czy jest możliwe jego obejście i zajęcie się pilniejszym problemem;
6) podejmowanie działań naprawczych – operator ma możliwość naprawienia szkód wyrządzonych przez incydent;
7) ograniczenie skutków incydentu – operator jest w stanie przywrócić stan normalnego działania.

18. Szerszym terminem od obsługi incydentu jest zarządzanie incydentem (art. 2 pkt 18 CyberbezpU), które dotyczy też kwestii organizacyjnych, tzn.:

1) wyszukiwania powiązań między incydentami – wynajdywania powiązań pomiędzy poszczególnymi elementami łańcuchu niszczenia intruza (ang. *kill chain*) poprzez wykrycie zależności między np. rodzajem ataku a sposobem dostarczenia złośliwego oprogramowania, czy też między różnymi incydentami (np. czy korzystają z tej samej podatności, co wskazuje na pilną konieczność jej likwidacji);
2) usuwania przyczyn wystąpienia incydentów – likwidacji podatności istniejących w posiadanym oprogramowaniu, podejmowanie czynności zmniejszających ryzyko wystąpienia incydentu w przyszłości, usuwanie wykrytych podatności;
3) opracowywania wniosków wynikających z obsługi incydentu – przejrzenie i ocena swojej działalności podczas obsługi incydentu, przejrzenie oprogramowania, procesów i procedur w zakresie bezpieczeństwa w celu poprawy poziomu bezpieczeństwa w przyszłości.

Obsługa incydentu jest obowiązkiem każdego operatora, dostawcy i podmiotu publicznego. Nie chodzi tu tylko o incydenty poważne, ale również incydenty zwykłe.

VI. Wokół ryzyka: ryzyko, szacowanie ryzyka zarządzanie ryzykiem, zagrożenie cyberbezpieczeństwa, podatność

19. Należy też wskazać na definicje związane z szacowaniem ryzyka i zagrożeniami. Ustawa definiuje ryzyko (art. 2 pkt 12 CyberbezpU), szacowanie ryzyka (art. 2 pkt 13 CyberbezpU), zarządzanie ryzykiem (art. 2 pkt 19 CyberbezpU), zagrożenie cyberbezpieczeństwa (art. 2 pkt 17 CyberbezpU) i podatność (art. 2 pkt 11 CyberbezpU). Podczas definiowania posłużono się Polskimi Normami, aby osiągnąć jak największą zgodność z terminologią stosowaną przez techników i inżynierów.

VII. Zespoły CSIRT

20. Ustawa definiuje też trzy zespoły CSIRT, umiejscowione odpowiednio przy Agencji Bezpieczeństwa Wewnętrznego, Ministrze Obrony Narodowej oraz Naukowej i Akademickiej Sieci Komputerowej – Państwowym Instytucie Badawczym. Zespoły CSIRT zostały opisane w komentarzu do art. 26.

VIII. Usługa kluczowa, usługa cyfrowa

21. W CyberbezpU zdefiniowano również usługę kluczową i cyfrową. Definicję usługi kluczowej należy czytać razem z przepisami dotyczącymi identyfikacji operatorów, dlatego ten temat zostanie rozwinięty w części dotyczącej obowiązków operatorów (zob. komentarz do art. 5). W tym miejscu warto jedynie wskazać, że w definicjach dyrektywy NIS nie zostało opisane, czym są usługi kluczowe – istnieje jedynie opis w art. 5

ust. 2 lit. a dyrektywy NIS – jest to usługa, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej i została określona w załączniku II do dyrektywy NIS.

22. Usługi cyfrowe w rozumieniu CyberbezpU (i dyrektywy NIS) są trzy:
1) internetowa platforma handlowa,
2) przetwarzanie w chmurze,
3) wyszukiwarka internetowa.

Należy wskazać na problem z tekstem dyrektywy NIS, który w polskiej wersji językowej używa terminu „platforma handlowa", podczas gdy patrząc na inne wersje językowe, lepszy byłby termin „targowisko". Przykładowo, w wersji angielskiej termin ten brzmi: „*Online marketplace*", w wersji niemieckiej: „*Online-Marktplatz*", hiszpańskiej: „*Mercado en línea*", niderlandzkiej: „*Onlinemarktplaats*", słowackiej: „*Online trhovisko*", a francuskiej: „*Place de marché en ligne*"). Ta usługa cyfrowa dotyczy platform, które udostępniają konsumentom i przedsiębiorcom handlowym możliwość zawierania umów sprzedaży lub umów o świadczenie usług online z przedsiębiorcami handlowymi i są ostatecznym miejscem zawierania tych umów (por. motyw 15 dyrektywy NIS). Spod reżimu ustawowego wyłączeni są pośrednicy, tacy jak porównywarki cenowe. Należy wskazać, że **za internetową platformę handlową w rozumieniu dyrektywy NIS nie mogą zostać uznane usługi świadczone przez przedsiębiorców w ramach sklepów internetowych, ponieważ nie realizują one przesłanki wskazanej w definicji, tj. umożliwienia zawarcia umowy z przedsiębiorcami** (*P. Gruszecki*, Obowiązki dostawców usług cyfrowych w świetle postanowień dyrektywy NIS – cz. 1, „Law2Business – Blog Kancelarii Kochański i Partnerzy", http://law2business.pl/2016/12/06/obowiazki-dostawcow-uslug-cyfrowych-swietle-postanowien-dyrektywy-nis-cz-1/, 2016 r., dostęp: 30.4.2019 r.). Dla uznania, że dany podmiot świadczy usługę cyfrową, nie ma znaczenia, czy oferuje on usługę, produkt fizyczny czy oprogramowanie (zob. również motyw 15 dyrektywy NIS).

23. Definicja usługi przetwarzania w chmurze została skonstruowana na podstawie terminów technologicznych, a nie prawnych, dlatego należy odczytywać ją razem z motywami dyrektywy NIS i definicją usługi cyfrowej. Usługa przetwarzania w chmurze dotyczy tylko usług świadczonych przez dany podmiot swoim klientom. Wyłączone są zatem przypadki chmury prywatnej, która jest usługą świadczoną do wewnątrz organizacji.

24. Warto wspomnieć, że w pierwotnym tekście projektu usługi cyfrowe miały obejmować: platformy handlu elektronicznego, internetowe portale płatnicze, portale społecznościowe, wyszukiwarki, usługi chmur obliczeniowych oraz sklepy z aplikacjami (Wniosek – Dyrektywa Parlamentu Europejskiego i Rady w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii /* COM/2013/048 final – 2013/0027 (COD) */). W trakcie procesu legislacyjnego usunięto internetowe portale płatnicze (uregulowane zmienioną dyrektywą PSD2), sklepy z aplikacjami (uznane przez Radę UE za rodzaj rynków, tj. platform online) oraz portale społecznościowe (zgodnie z porozumieniem politycznym osiągniętym przez Parlament Europejski i Radę) [komunikat Komisji do