Cyberbezpieczeństwo – kluczowe wyzwania dla samorządu

Po wyjątkowo długim procesie legislacyjnym ustawa o krajowym systemie cyberbezpieczeństwa wreszcie została uchwalona. Jej wdrożenie stawia przed jednostkami samorządu terytorialnego wiele wyzwań organizacyjnych i regulacyjnych. Część z nich zostanie zasygnalizowana w tym materiale.

DZP
więcej niż prawo

WOJCIECH DZIOMDZIORA

radca prawny, Counsel w kancelarii Domański, Zakrzewski, Palinka

Stale rosnący wpływ technologii teleinformatycznych na rozwój społeczno-gospodarczy oraz wzrost ich wykorzystania sprawia, że oferowane produkty i usługi są obecnie coraz silniej zależne od zapewnienia cyberbezpieczeństwa.

O skali zagrożeń, jakie wiążą się z rozwojem internetu, świadczą statystyki publikowane przez zespoły CERT (zespoły reagowania na incydenty komputerowe). W 2016 roku CERT Polska działający w NASK – Państwowym Instytucie Badawczym obsłużył 1926 incydentów, tj. o 32% więcej niż w 2015 roku. Do najczęściej zgłaszanych należą następujące kategorie incydentów: oszustwa komputerowe (55,5%), obraźliwe i nielegalne treści (12,31%), złośliwe oprogramowanie (10,96%), próby włamań (5,66%), gromadzenie informacji (3,37%), włamania (2,8%), dostępność zasobów (2,34%), atak na bezpieczeństwo informacji (2,34%), inne (4,72%).

6 lipca 2016 r. przyjęto dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii. Zawarte w jej treści regulacje wdraża do polskiego porządku prawnego uchwalona 5 lipca 2018 r. ustawa o krajowym systemie cyberbezpieczeństwa (dalej: ustawa).

Adresat: podmioty publiczne

Przepisy ustawy definiują cyberbezpieczeństwo jako „odporność systemów informacyjnych na wszelkie działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy". W tej definicji najważniejsze jest określenie przedmiotu ochrony – tj. danych lub związanych z nimi usług. Co prawda nie zdefiniowano w ustawie, czym są dane, ale uznać trzeba, że chodzi o wszelkiego rodzaju dane podlegające ochronie i te, na podstawie których świadczone są różnorakie usługi.

WAŻNE

Cyberbezpieczeństwo to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

Ustawa dotyczy przede wszystkim przedsiębiorców zaliczonych do grupy tzw. operatorów usług kluczowych, czyli najważniejszych przedsiębiorstw z sektora energii, transportu, bankowości i infrastruktury rynków finansowych, ochrony zdrowia, zaopatrzenia w wodę pitną i infrastruktury cyfrowej. Mniejszy zakres obowiązków dotyczy dostawców usług cyfrowych, tj. dostarczycieli internetowych platform handlowych, usług przetwarzania w chmurze oraz wyszukiwarek internetowych.

Jednakże **najliczniejszą grupą podmiotów objętych nowymi obowiązkami ustawowymi będą podmioty publiczne,** w tym m.in.: jednostki sektora finansów publicznych, instytuty badawcze; NBP, BGK, Urząd Dozoru Technicznego; Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkie fundusze ochrony środowiska i gospodarki wodnej, a także spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicz-

nej. To grupa bardzo liczna, obejmująca całą administrację, samorządy terytorialne i spółki komunalne.

Zadania dla samorządów

Pierwszym zadaniem będzie **wyznaczenie osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.** Powinna nią być osoba, która odpowiada w urzędzie za bezpieczeństwo systemów teleinformatycznych i bezpieczeństwo informacji. Szczególnie w małych jednostkach, z uwagi na ograniczoną ilość obowiązków, mogą to być te same osoby, które pełnią funkcję inspektorów ochrony danych.

Zgodnie z przyjętymi przepisami, jednostka samorządu terytorialnego będzie mogła wyznaczyć jedną osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa dla jej wszystkich jednostek organizacyjnych i przekazanie danych kontaktowych tej osoby do właściwego CSIRT.
Jednakże wyznaczenie osoby kontaktowej to za mało. Konieczne będzie przygotowanie struktur i procedur, które pozwolą zrealizować następujące obowiązki:

1) zapewnienie zarządzania incydentem, tj. zapewnienie obsługi incydentu, wyszukiwania powiązań między incydentami, usuwania przyczyn ich wystąpienia oraz opracowania wniosków z obsługi incydentu,
2) zgłoszenie incydentu do właściwego CSIRT w czasie do 24 godzin od momentu jego wykrycia,
3) zapewnienie obsługi incydentu i incydentu krytycznego we współpracy z właściwym CSIRT poprzez przekazanie niezbędnych danych, w tym danych osobowych,
4) zapewnienie osobom, na rzecz których dana jednostka samorządu terytorialnego realizuje zadania publiczne, dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami; wspomniany dostęp do wiedzy powinien być realizowany w szczególności przez publikowanie informacji w tym zakresie na stronie internetowej jednostki.

Jednostki samorządu terytorialnego muszą dodatkowo pamiętać, że ustawie o krajowym systemie cyberbezpieczeństwa w sposób szczególny podlegają również podmioty nadzorowane przez te jednostki lub takie, w których te jednostki posiadają udziały. Dotyczy to w szczególności przedsiębiorców, którzy mogą być zaliczeni do kategorii operatorów usług kluczowych. Jak wspomniałem wcześniej, będą to przedsiębiorcy z następujących sektorów: energii, transportu, bankowości i infrastruktury rynków finansowych, ochrony zdrowia, zaopatrzenia w wodę pitną i infrastruktury cyfrowej. O jakich zatem mówimy przedsiębiorcach w kontekście jednostek samorządu terytorialnego? Mogą to być szpitale, przedsiębiorstwa wodno-kanalizacyjne, operatorzy lotnisk. To na takich przedsiębiorcach spoczywać będzie najwięcej obowiązków związanych z budowaniem cyberbezpieczeństwa.

SŁOWNICZEK

Skrótem **CSIRT** określa się Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego. Przepisy ustawy wyróżniają trzy zespoły CSIRT:

- CSIRT GOV – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego,
- CSIRT MON – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Ministra Obrony Narodowej,
- CSIRT NASK – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy.

Procedura zgłaszania incydentu (zdarzenia mogącego mieć negatywny wpływ na cyberbezpieczeństwo)

Incydent w podmiocie publicznym zgłasza się niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia. Zgłoszenie powinno zawierać:

1) dane podmiotu zgłaszającego, w tym nazwę podmiotu, numer we właściwym rejestrze, siedzibę i adres;
2) imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby składającej zgłoszenie;
3) imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji;
4) opis wpływu incydentu w podmiocie publicznym na realizowane zadanie publiczne, w tym:
   a) wskazanie zadania publicznego, na które incydent miał wpływ,
   b) liczbę osób, na które incydent miał wpływ,
   c) moment wystąpienia i wykrycia incydentu oraz czas jego trwania,
   d) zasięg geograficzny obszaru, którego dotyczy incydent,
   e) przyczynę zaistnienia incydentu i sposób jego przebiegu oraz skutki jego oddziaływania na systemy informacyjne podmiotu publicznego;
5) informacje o przyczynie i źródle incydentu;
6) informacje o podjętych działaniach zapobiegawczych;
7) informacje o podjętych działaniach naprawczych;
8) inne istotne informacje.

W zgłoszeniu podmiot publiczny oznacza informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa.

Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV może zwrócić się do podmiotu publicznego o uzupełnienie zgłoszenia o informacje, w tym informacje stanowiące tajemnice prawnie chronione, w zakresie niezbędnym do realizacji zadań, o których mowa w ustawie.

Koordynacja z przepisami innych ustaw

Przed jednostkami samorządu terytorialnego stanie również wyzwanie **skoordynowania obowiązków wynikających z przepisów nowej ustawy o cyberbezpieczeństwie z obowiązkami wynikającymi z innych przepisów,** w szczególności z RODO, ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne (w tym aktu wykonawczego do tej ustawy – Krajowych Ram Interoperacyjności czy ustawy o ochronie informacji niejawnych. Wszystkie te przepisy (a także kilka innych) splatają się ze sobą i wzajemnie się przenikają. Ważne jest, aby nie traktować ich odrębnie. Bezpieczeństwo systemów teleinformatycznych, zarządzanie i ochrona informacji, a także ochrona danych osobowych muszą tworzyć spójny system.

Co zatem należy czynić? Przede wszystkim zachować spokój i zdrowy rozsądek. Nie ulegać histerii oraz nie słuchać marnych, ale hałaśliwych doradców, co stało się powszechnym zjawiskiem w przypadku RODO. Należy pamiętać, że wdrożenie odpowiednich systemów bezpieczeństwa nie może służyć jedynie spełnieniu formalnych wymogów stawianych przez prawo, ale ma przede wszystkim zabezpieczać organizację przed atakami cybernetycznymi.

Każda organizacja, w szczególności podmioty publiczne, takie jak samorząd terytorialny, musi być przygotowana nie tylko do odparcia ataków cybernetycznych, ale również do działania w sytuacji, kiedy atak cybernetyczny się powiedzie. Poważne incydenty cybernetyczne mogą mieć szerokie konsekwencje finansowe, prawne i wizerunkowe. Dlatego cyberbezpieczeństwo już dawno przestało być domeną jedynie działów IT i wyspecjalizowanych komórek ds. bezpieczeństwa. W system cyberbezpieczeństwa muszą być włączone również służby prawne, odpowiedzialne za komunikację zewnętrzną oraz zarządzający daną jednostką. Zarządzający jednostkami samorządu terytorialnego muszą zdać sobie sprawę, że cyberbezpieczeństwo już dziś jest jednym z najważniejszych tematów, jakim powinni poświęcać swoją uwagę i czas. ©℗

Podstawa prawna

► art. 21 – 25 ustawy z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560)