ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2018/151

z dnia 30 stycznia 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

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii ([1]), w szczególności jej art. 16 ust. 8,

a także mając na uwadze, co następuje:

(1) Zgodnie z dyrektywą (UE) 2016/1148 dostawcy usług cyfrowych mogą przedsięwziąć środki techniczne i organizacyjne, jakie uznają za właściwe i proporcjonalne, aby zarządzać ryzykiem, na jakie narażone jest bezpieczeństwo ich sieci i systemów informatycznych, o ile środki te zapewniają odpowiedni poziom bezpieczeństwa i uwzględniają elementy przewidziane we wspomnianej dyrektywie.

(2) Przy określaniu właściwych i proporcjonalnych środków technicznych i organizacyjnych dostawcy usług cyfrowych powinni podchodzić do kwestii bezpieczeństwa informacji w sposób systematyczny, stosując podejście oparte na analizie ryzyka.

(3) W celu zapewnienia bezpieczeństwa systemów i obiektów dostawcy usług cyfrowych powinni stosować procedury oceny i analizy. Działania te powinny dotyczyć systematycznego zarządzania sieciami i systemami informatycznymi, bezpieczeństwa fizycznego i środowiskowego, bezpieczeństwa dostaw oraz kontroli dostępu.

(4) Należy zachęcać dostawców usług cyfrowych, aby podczas przeprowadzania analizy ryzyka w kontekście systematycznego zarządzania sieciami i systemami informatycznymi dokonywali identyfikacji konkretnych rodzajów ryzyka oraz wskazywali ich wagę, na przykład przez określenie zagrożeń dla krytycznych aktywów i tego, jak mogą one wpłynąć na operacje, oraz przez ustalenie najlepszych sposobów złagodzenia tych zagrożeń w oparciu o aktualne możliwości i potrzeby w zakresie zasobów.

(5) Polityki w zakresie zasobów ludzkich mogą odnosić się do zarządzania umiejętnościami, w tym do aspektów dotyczących rozwoju umiejętności związanych z bezpieczeństwem oraz podnoszenia świadomości. Należy zachęcać dostawców usług cyfrowych do uwzględnienia – przy podejmowaniu decyzji w sprawie zestawu polityk w zakresie bezpieczeństwa operacji – aspektów dotyczących zarządzania zmianami, zarządzania podatnością na zagrożenia, sformalizowania praktyk operacyjnych i administracyjnych oraz mapowania systemu.

(6) Polityki w zakresie architektury bezpieczeństwa mogą obejmować w szczególności rozdzielenie sieci i systemów, jak również szczególne środki bezpieczeństwa dotyczące operacji krytycznych, takich jak operacje administrowania. Rozdzielenie sieci i systemów mogłoby umożliwić dostawcy usług cyfrowych dokonanie rozróżnienia między elementami, takimi jak przepływy danych i zasoby obliczeniowe, które należą do klienta, grupy klientów, dostawcy usług cyfrowych lub stron trzecich.

(7) Środki przedsięwzięte w odniesieniu do bezpieczeństwa fizycznego i środowiskowego powinny zabezpieczać sieci i systemy informatyczne organizacji przed szkodami powodowanymi przez takie incydenty, jak kradzież, pożar, powódź lub inne czynniki pogodowe, awarie systemów telekomunikacyjnych lub awarie zasilania.

(8) Bezpieczeństwo dostaw w zakresie energii elektrycznej, paliw lub energii chłodniczej może obejmować bezpieczeństwo łańcucha dostaw, co uwzględnia w szczególności bezpieczeństwo wykonawców i podwykonawców zewnętrznych oraz zarządzanie nimi. Identyfikowalność krytycznych dostaw dotyczy zdolności dostawców usług cyfrowych do ustalania i rejestrowania źródeł tych dostaw.

(9) Kategoria użytkowników usług cyfrowych powinna obejmować osoby fizyczne lub prawne, które są klientami lub abonentami internetowej platformy handlowej lub usługi przetwarzania w chmurze bądź które odwiedzają stronę wyszukiwarki internetowej w celu przeprowadzenia wyszukiwania przy pomocy słów kluczowych.

([1]) Dz.U. L 194 z 19.7.2016, s. 1.

(10) Ustalając istotność wpływu incydentu, przypadki określone w niniejszym rozporządzeniu należy traktować jako niewyczerpujący wykaz istotnych incydentów. Należy wyciągnąć wnioski z wykonania niniejszego rozporządzenia oraz z działalności grupy współpracy w odniesieniu do kwestii gromadzenia informacji z zakresu najlepszych praktyk dotyczących ryzyk i incydentów oraz dyskusji na temat zasad dotyczących sprawozdawczości w zakresie zgłaszania incydentów, o których mowa art. 11 ust. 3 lit. i) oraz m) dyrektywy (UE) 2016/1148. Wynikiem mogą być kompleksowe wytyczne dotyczące progów ilościowych dla parametrów zgłoszeń, które mogą prowadzić do powstania obowiązku zgłoszenia dla dostawców usług cyfrowych zgodnie z art. 16 ust. 3 dyrektywy (UE) 2016/1148. W stosownych przypadkach Komisja może również rozważyć dokonanie przeglądu progów aktualnie przewidzianych w niniejszym rozporządzeniu.

(11) Aby umożliwić właściwym organom uzyskanie informacji na temat potencjalnych nowych rodzajów ryzyka, dostawców usług cyfrowych należy zachęcać do dobrowolnego zgłaszania wszelkich incydentów, których cechy były im wcześniej nieznane, takich jak nowe *exploity*, wektory ataku lub podmioty zagrażające bezpieczeństwu, słabe punkty i zagrożenia.

(12) Niniejsze rozporządzenie powinno być stosowane od dnia następującego po upływie terminie transpozycji dyrektywy (UE) 2016/1148.

(13) Środki przewidziane w niniejszym rozporządzeniu są zgodne z opinią Komitetu ds. Bezpieczeństwa Sieci i Systemów Informatycznych, o którym mowa w art. 22 dyrektywy (UE) 2016/1148,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Przedmiot

W niniejszym rozporządzeniu doprecyzowano elementy, jakie mają zostać uwzględnione przez dostawców usług cyfrowych przy określaniu i przedsiębraniu środków mających na celu zapewnienie poziomu bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez nich w kontekście oferowania usług, o których mowa w załączniku III do dyrektywy (UE) 2016/1148, jak również parametry, które należy wziąć pod uwagę w celu ustalenia, czy incydent ma istotny wpływ na świadczenie tych usług.

Artykuł 2

Zabezpieczenia

1. Bezpieczeństwo systemów i obiektów, o których mowa w art. 16 ust. 1 lit. a) dyrektywy (UE) 2016/1148, oznacza bezpieczeństwo sieci i systemów informatycznych oraz ich środowiska fizycznego i obejmuje następujące elementy:

a) systematyczne zarządzanie sieciami i systemami informatycznymi, co oznacza mapowanie systemów informatycznych oraz ustanowienie zestawu odpowiednich polityk w zakresie zarządzania bezpieczeństwem informacji, w tym analiz ryzyka, zasobów ludzkich, bezpieczeństwa operacji, architektury bezpieczeństwa, zabezpieczenia danych i zarządzania cyklem życia systemu oraz, w stosownych przypadkach, szyfrowania i zarządzania nim;

b) bezpieczeństwo fizyczne i środowiskowe, które oznacza dostępność zestawu środków mających na celu ochronę bezpieczeństwa sieci i systemów informatycznych dostawców usług cyfrowych przed szkodami z zastosowaniem całościowego podejścia do kwestii zagrożeń opartego na analizie ryzyka, które uwzględnia np. awarie systemu, błędy ludzkie, działania złośliwe bądź zjawiska naturalne;

c) bezpieczeństwo dostaw oznacza ustanowienie oraz utrzymywanie odpowiednich polityk w celu zagwarantowania dostępności oraz, w stosownych przypadkach, identyfikowalności krytycznych dostaw wykorzystywanych do świadczenia usług;

d) kontrole dostępu do sieci i systemów informatycznych, co oznacza dostępność zestawu środków, które mają zagwarantować, że dostęp fizyczny i dostęp logiczny do sieci i systemów informatycznych, w tym administracyjne bezpieczeństwo sieci i systemów informatycznych, są uprawnione i ograniczone w oparciu o wymogi dotyczące prowadzenia działalności i bezpieczeństwa.

2. W odniesieniu do postępowania w przypadku incydentu, o którym mowa w art. 16 ust. 1 lit. b) dyrektywy (UE) 2016/1148, środki przedsiębrane przez dostawcę usług cyfrowych obejmują:

a) utrzymywanie i testowanie procesów oraz procedur wykrywania w celu zapewnienia terminowej i odpowiedniej wiedzy na temat nietypowych zdarzeń;

b) procesy i polityki dotyczące zgłaszania incydentów oraz identyfikowania niedociągnięć i słabych punktów w jego systemach informatycznych;

c) reagowanie zgodnie z ustanowionymi procedurami oraz składanie sprawozdań z wyników przedsięwziętych środków;

d) ocenę powagi danego incydentu, dokumentowanie wiedzy uzyskanej z analizy incydentów oraz gromadzenie odpowiednich informacji, które mogą stanowić dowody i wspierać proces ciągłego doskonalenia.

3. Zarządzanie ciągłością działania, o którym mowa w art. 16 ust. 1 lit. c) dyrektywy (UE) 2016/1148, oznacza zdolność organizacji do utrzymania lub, w razie potrzeby, przywrócenia realizacji usług na uprzednio określonych dopuszczalnych poziomach, po wystąpieniu zakłócenia, i obejmuje:

a) ustanowienie i stosowanie planów awaryjnych w oparciu o analizę wpływu na działalność w celu zapewnienia ciągłości usług świadczonych przez dostawców usług cyfrowych, co jest oceniane i testowane w regularnych odstępach czasu, na przykład przez ćwiczenia;

b) zdolności w zakresie przywracania gotowości do pracy po katastrofie, które są oceniane i testowane w regularnych odstępach czasu, na przykład przez ćwiczenia.

4. Monitorowanie, audyt i testowanie, o których mowa w art. 16 ust. 1 lit. d) dyrektywy (UE) 2016/1148, obejmują ustanowienie i utrzymywanie polityk w zakresie:

a) przeprowadzania zaplanowanej sekwencji obserwacji lub pomiarów w celu dokonania oceny, czy sieci i systemy informatyczne działają zgodnie z zamierzeniem;

b) inspekcji i weryfikacji mających na celu sprawdzenie, czy stosuje się normę lub zbiór wytycznych, czy rejestry są dokładne, a także czy realizowane są cele w zakresie efektywności i skuteczności;

c) procesu mającego na celu ujawnienie wad mechanizmów bezpieczeństwa sieci i systemów informatycznych, które służą ochronie danych i utrzymaniu funkcjonalności zgodnie z zamierzeniem. Tego rodzaju proces obejmuje procesy techniczne i personel zaangażowany w przepływ operacji.

5. Normy międzynarodowe, o których mowa w art. 16 ust. 1 lit. e) dyrektywy (UE) 2016/1148, oznaczają normy przyjęte przez międzynarodową jednostkę normalizacyjną, o której mowa w art. 2 ust. 1 lit. a) rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1025/2012 ([1]). Zgodnie z art. 19 dyrektywy (UE) 2016/1148 stosowane mogą być również europejskie lub uznane międzynarodowe normy i specyfikacje mające znaczenie dla bezpieczeństwa sieci i systemów informatycznych, w tym istniejące normy krajowe.

6. Dostawcy usług cyfrowych zapewniają udostępnianie właściwemu organowi odpowiedniej dokumentacji do celów weryfikacji zgodności z zabezpieczeniami określonymi w ust. 1, 2, 3, 4 i 5.

Artykuł 3

Parametry, jakie należy wziąć pod uwagę w celu określenia, czy wpływ incydentu jest istotny

1. Jeśli chodzi o liczbę użytkowników, których dotyczy incydent, w szczególności użytkowników zależnych od usługi na potrzeby świadczenia ich własnych usług, o których mowa w art. 16 ust. 4 lit. a) dyrektywy (UE) 2016/1148, dostawca usług cyfrowych musi być w stanie oszacować jedną z następujących liczb:

a) liczbę dotkniętych incydentem osób fizycznych i osób prawnych, z którymi zawarto umowę na świadczenie danej usługi; lub

b) liczbę dotkniętych incydentem użytkowników, którzy korzystali z tej usługi, w oparciu w szczególności o wcześniejsze dane o ruchu.

2. Czas trwania incydentu, o którym mowa w art. 16 ust. 4 lit. b), oznacza okres, jaki upływa od zakłócenia prawidłowego świadczenia usługi pod względem jej dostępności, autentyczności, integralności lub poufności, do czasu przywrócenia stanu normalnego.

3. Jeśli chodzi o zasięg geograficzny związany z obszarem, którego dotyczy incydent, o którym mowa w art. 16 ust. 4 lit. c) dyrektywy (UE) 2016/1148, dostawca usług cyfrowych musi być w stanie ustalić, czy dany incydent ma wpływ na świadczenie jego usług w poszczególnych państwach członkowskich.

4. Zasięg zakłócenia funkcjonowania usługi, o którym mowa w art. 16 ust. 4 lit. d) dyrektywy (UE) 2016/1148, mierzy się w odniesieniu do jednego lub większej liczby następujących aspektów osłabionych w wyniku danego incydentu: dostępność, autentyczność, integralność lub poufność danych lub powiązanych usług.

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1025/2012 z dnia 25 października 2012 r. w sprawie normalizacji europejskiej, zmieniające dyrektywy Rady 89/686/EWG i 93/15/EWG oraz dyrektywy Parlamentu Europejskiego i Rady 94/9/WE, 94/25/WE, 95/16/WE, 97/23/WE, 98/34/WE, 2004/22/WE, 2007/23/WE, 2009/23/WE i 2009/105/WE oraz uchylające decyzję Rady 87/95/EWG i decyzję Parlamentu Europejskiego i Rady nr 1673/2006/WE (Dz.U. L 316 z 14.11.2012, s. 12).

5. W odniesieniu do zasięgu wpływu na działalność gospodarczą i społeczną, o którym mowa w art. 16 ust. 4 lit. e) dyrektywy (UE) 2016/1148, dostawca usług cyfrowych musi być w stanie – w oparciu o wskazówki, takie jak charakter jego stosunków umownych z klientem lub, w stosownych przypadkach, potencjalna liczba użytkowników dotkniętych incydentem – stwierdzić, czy incydent spowodował znaczne straty materialne bądź niematerialne dla użytkowników, na przykład odnośnie do zdrowia, bezpieczeństwa lub uszkodzenia mienia.

6. Do celów ust. 1, 2, 3, 4 i 5 od dostawców usług cyfrowych nie wymaga się zbierania dodatkowych informacji, do których nie mają oni dostępu.

Artykuł 4

Istotny wpływ incydentu

1. Dany incydent uznaje się za mający istotny wpływ, jeżeli zaistniała co najmniej jedna z następujących sytuacji:

a) usługa świadczona przez dostawcę usług cyfrowych była niedostępna przez ponad 5 000 000 użytkownikogodzin, przy czym pojęcie „użytkownikogodziny" odnosi się do liczby dotkniętych incydentem użytkowników w Unii przez okres sześćdziesięciu minut;

b) incydent doprowadził do utraty integralności, autentyczności lub poufności przechowywanych lub przekazywanych bądź przetwarzanych danych lub powiązanych usług, oferowanych bądź dostępnych poprzez sieci i systemy informatyczne dostawcy usług cyfrowych, która dotknęła ponad 100 000 użytkowników w Unii;

c) incydent spowodował ryzyko dla bezpieczeństwa publicznego lub ryzyko wystąpienia ofiar śmiertelnych;

d) incydent wyrządził co najmniej jednemu użytkownikowi w Unii stratę materialną, której wysokość przekracza 1 000 000 EUR.

2. Opierając się na najlepszych praktykach zebranych przez grupę współpracy w wyniku realizacji jej zadań zgodnie z art. 11 ust. 3 dyrektywy (UE) 2016/1148 oraz na podstawie dyskusji wynikających z jej art. 11 ust. 3 lit. m), Komisja może dokonać przeglądu progów określonych w ust. 1.

Artykuł 5

Wejście w życie

1. Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

2. Niniejsze rozporządzenie stosuje się od dnia 10 maja 2018 r.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia 30 stycznia 2018 r.

W imieniu Komisji
Jean-Claude JUNCKER
Przewodniczący