Jakie bedzie ostateczne brzmienie Dyrektywy NIS 2?

Piotr Studziński-Raczyński
Starszy Specjalista ds. DNS

Czym dyrektywa NIS 2 różni się od swojej poprzedniczki? Dyrektywa Parlamentu Europejskiego i Rady (UE) w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa, rozszerzając w sposób znaczący zakres dotychczas objętych nią podmiotów, dzieli je na: podmioty kluczowe (*essential entities*) i podmioty ważne (*important entities*). Istotną zmianą jest również objęcie sektora komunikacji elektronicznej w ramy jednolitego systemu prawnego w całej Unii Europejskiej. Taki stan rzeczy wydaje się naturalną konsekwencją rozwoju technologicznego, którego efektem jest rosnący udział usług świadczonych drogą elektroniczną.

W związku z prowadzonymi przez Kancelarię Prezesa Rady Ministrów konsultacjami projektu dyrektywy NIS 2, zakładającego aktualizację regulacji dot. bezpieczeństwa sieci i systemów informatycznych, Rada ds. Cyfryzacji zgadza się co do zasady z ogólnym kierunkiem objęcia regulacją kluczowych sektorów - w tym w szczególności telekomunikacyjnego oraz administracji publicznej - co umożliwi ujednolicenie zasad cyberbezpieczeństwa zarówno na poziomie UE, jak i krajowym. Rada zwraca również uwagę, iż projekt dyrektywy NIS 2 powinien być rozpatrywany także po kątem nowej strategii cyberbezpieczeństwa – „Zaufanie i bezpieczeństwo w centrum cyfrowej dekady" (*The EU's Cybersecurity Strategy for the Digital Decade*), zakładającej analizę dostępnych do wdrożenia przez UE rozwiązań legislacyjnych. Celem takiej analizy byłoby rozszerzenie możliwości, kompetencji i zasobów UE, a w rezultacie doprowadzenie do osiągnięcia satysfakcjonującego poziomu suwerenności technologicznej.

Projekt dyrektywy NIS 2 w motywie 15. wskazuje, że utrzymywanie bezpiecznego systemu DNS jest zasadnicze dla utrzymania integralności i stabilności działania Internetu. Z perspektywy tej oceny postuluje się również, że ważne jest zapewnienie aktualnych danych abonentów („dane WHOIS") oraz bezpiecznego dostępu do takich danych, co z kolei przekłada się na utrzymanie wysokiego wspólnego poziomu cyberbezpieczeństwa w UE. Art. 23 projektu dyrektywy NIS 2 zobowiązuje Państwa Członkowskie, aby dane dotyczące abonentów nazw domen były aktualne i kompletne oraz gromadzone i przechowywane przez rejestry i rejestratorów TLD z należytą starannością. Odnosząc postanowienia art. 23 do wyżej wspomnianej idei utrzymania wysokiego wspólnego poziomu cyberbezpieczeństwa w UE, dbałość o aktualne i kompletne dane abonentów może wpływać np. na ograniczenie liczby ataków z wykorzystaniem nazw domen w celu podszywania się np. pod banki, dostawców energii czy usług kurierskich.

3 maja 2021 roku, Komisja Przemysłu, Badań Naukowych i Energii Parlamentu Europejskiego (ITRE) wydała projekt sprawozdania w sprawie wniosku dotyczącego dyrektywy NIS 2. W odniesieniu do obowiązku utrzymywania dokładnych danych rejestracyjnych nałożonego na rejestry i rejestratorów nazw domen, projekt sprawozdania dodaje kryterium ich weryfikacji. Zgodnie z projektem sprawozdania ITRE, rejestry i rejestratorzy nazw domen powinni dążyć do zapewnienia integralności i dostępności danych rejestracyjnych poprzez wdrożenie odpowiednich środków technicznych i organizacyjnych, np. procesu potwierdzania danych rejestracyjnych przez abonentów. Jeśli chodzi o dostęp do tych danych, projekt sprawozdania sugeruje, że rejestry i rejestratorzy powinni odpowiadać na wnioski o udostępnienie danych rejestracyjnych w cią-

gu 72 godzin. Sugerowane jest również włączenie definicji usług rejestracji nazw domen, która obejmuje usługi świadczone przez rejestry i rejestratorów, dostawców usług typu privacy/proxy, pośredników lub odsprzedawców (resellers) oraz wszelkie inne usługi, które są związane z rejestracją nazw domen. W projekcie sprawozdania ITRE określono także, iż odpowiednie informacje, które rejestry, rejestratorzy i inne podmioty świadczące usługi rejestracji nazw domen gromadzą i utrzymują jako dokładne, kompletne i zweryfikowane, powinny obejmować co najmniej imię i nazwisko abonenta, adres fizyczny, adres poczty elektronicznej, jak również numer telefonu. Powyższe dotyczyć miałoby zarówno danych osób fizycznych jak i prawnych. Projekt sprawozdania ITRE będzie podstawą głównego stanowiska Parlamentu w sprawie projektu dyrektywy NIS 2. Na szczególną uwagę w projekcie sprawozdania w odniesieniu do ccTLD zasługuje propozycja obowiązku weryfikacji danych rejestracyjnych. Zgodnie z pkt. 59 sprawozdania, procesy weryfikacji powinny odzwierciedlać obecnie najlepsze praktyki stosowane w branży (w tym system identyfikacji elektronicznej eID).

3 czerwca 2021 roku, Komisja Europejska przedstawiła swój wniosek dotyczący rozporządzenia w sprawie europejskiej tożsamości cyfrowej (EUID). Wniosek w sprawie EUID nakłada na Państwa Członkowskie obowiązek wydawania portfela europejskiej tożsamości cyfrowej w ramach zgłoszonego systemu identyfikacji elektronicznej (Krajowy Schemat Identyfikacji Elektronicznej), po przeprowadzeniu obowiązkowej oceny zgodności i dobrowolnej certyfikacji w ramach europejskiej certyfikacji bezpieczeństwa cybernetycznego na mocy unijnego aktu prawnego dotyczącego bezpieczeństwa cybernetycznego. Ponieważ obecne ramy eIDAS nie osiągnęły zamierzonego celu, jakim było zapewnienie funkcjonowania transgranicznych systemów identyfikacji elektronicznej we wszystkich państwach członkowskich*, we wniosku w sprawie EUID nałożono na Państwa Członkowskie wymóg zgłoszenia co najmniej jednego systemu identyfikacji elektronicznej. Aby zagwarantować, że użytkownicy mogą zidentyfikować, kto stoi za daną stroną internetową, we wniosku w sprawie EUID zawarto wymóg, aby dostawcy przeglądarek internetowych ułatwiali korzystanie z certyfikatów kwalifikowanych na potrzeby uwierzytelniania stron internetowych. Jeśli chodzi zaś o korzystanie z europejskich portfeli identyfikacji cyfrowej przez podmioty prywatne, wymagana jest zgoda dostawców infrastruktury cyfrowej na korzystanie z takich portfeli w celu świadczenia usług, w przypadku których silne uwierzytelnienie użytkownika na potrzeby identyfikacji online jest wymagane na mocy prawa krajowego lub unijnego lub na mocy zobowiązania umownego. Wniosek Komisji Europejskiej w sprawie EUID jest bardzo istotny w kontekście toczących się dyskusji na temat danych rejestracyjnych w ramach projektu dyrektywy NIS 2 oraz obowiązku KYBC „poznania swojego klienta" w zakresie wniosku w sprawie DSA (*Digital Services Act*), który może wymagać od rejestrów weryfikacji danych rejestracyjnych abonentów nazw domen. Wniosek KE w sprawie EUID ma na celu zapewnienie, aby wszystkie Państwa Członkowskie posiadały co najmniej jeden funkcjonujący system identyfikacji elektronicznej.

W odniesieniu do wspomnianej wyżej relacji projektu dyrektywy NIS 2 z założeniami nowej strategii cyberbezpieczeństwa, należy zauważyć, że 10 czerwca 2021 roku Parlament Europejski przyjął rezolucję w sprawie strategii bezpieczeństwa cybernetycznego UE, w której wzywa, między innymi, do stworzenia nowych solidnych ram bezpieczeństwa dla infrastruktur krytycznych UE w celu ochrony interesów bezpieczeństwa UE. W rezolucji wezwano Komisję Europejską do przygotowania przepisów mających na celu zapewnienie dostępności, osiągalności i integralności Internetu, a tym samym stabilności cyberprzestrzeni, w szczególności w odniesieniu do dostępu UE do globalnego systemu DNS. W rezolucji z zadowoleniem przyjęto również wniosek w sprawie europejskiego systemu nazw domen (DNS4EU) jako elementu wpływającego na od-

* W przypadku rejestrów domen internetowych konflikt techniczny polega na połączeniu identyfikatora eIDAS z identyfikatorem osobistym lokalnego systemu identyfikacji elektronicznej eID na poziomie krajowym.

porność Internetu. Zwrócono się również do Komisji o ocenę, w jaki sposób DNS4EU mógłby wykorzystywać najnowsze technologie, protokoły bezpieczeństwa i wiedzę fachową na temat zagrożeń cybernetycznych, aby zapewnić wszystkim Europejczykom szybki, bezpieczny i odporny system DNS. W rezolucji wskazano na konieczność lepszej ochrony protokołu BGP oraz podkreślono, że państwa UE powinny przyspieszyć wdrażanie IPv6. Promowany jest także model otwartego oprogramowania (open source), który - często jako podstawa funkcjonowania wielu gałęzi Internetu - okazał się skuteczny i efektywny. W kontekście opisanej powyżej zależności, należy pamiętać, że chociaż rezolucje Parlamentu Europejskiego nie są wiążącymi instrumentami prawnymi, zapewniają jednak ogólny kierunek działań Parlamentu w różnych obszarach polityki.

10 czerwca 2021 Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych Parlamentu Europejskiego (LIBE) wydała projekt opinii w sprawie wniosku dotyczącego dyrektywy NIS 2. Projekt opinii uwzględnia liczne zalecenia przedstawione przez EIOD (Europejski Inspektor Ochrony Danych) w zakresie strategii bezpieczeństwa cybernetycznego UE i projektu dyrektywy NIS 2. W odniesieniu do obowiązku dokładności danych rejestracyjnych, mającego zastosowanie wobec rejestrów i rejestratorów nazw domen, w projekcie opinii proponuje się wprowadzenie zmian dotyczących kategorii danych podlegających publikacji w zakresie osób prawnych oraz ogranicza się listę uprawnionych podmiotów ubiegających się o dostęp do danych abonenta do właściwych organów krajowych, w tym m.in. organów ścigania, zespołów CERT/CSIRT i organów ochrony danych osobowych. Zmiany proponowane w projekcie opinii, podobnie jak w sprawozdaniu ITRE, określają również, że istotne informacje gromadzone przez rejestry i rejestratorów powinny zawierać nazwisko, adres fizyczny, adres e-mail i numer telefonu abonenta nazwy domen. Poprawki zaproponowane w projekcie opinii LIBE wydają się być jednymi z bardziej wyważonych, ponieważ stanowią próbę odpowiedzi na obawy zgłoszone przez EIOD.

Swoje uwagi nt. projektu dyrektywy NIS 2 przedstawiła również Komisja Rynku Wewnętrznego i Ochrony Konsumentów Parlamentu Europejskiego (IMCO). 14 lipca 2021 roku członkowie ww. Komisji przyjęli opinię dotyczącą omawianej dyrektywy. Opinia IMCO, podobnie jak sprawozdanie ITRE, sugeruje poprawki mające na celu włączenie do art. 23 dostawców usług typu privacy/proxy, brokerów domen internetowych lub resellerów oraz wszelkich innych usług, które są związane z rejestracją nazw domen. Niektóre poprawki mają na celu dalsze dostosowanie zobowiązań dotyczących dokładności gromadzonych danych do GDPR. Zgodnie z opinią IMCO, obowiązek dokładności danych, określony w art. 23, powinien zostać rozszerzony o dodatkowy obowiązek weryfikacji danych w zakresie istotnych informacji niezbędnych do identyfikacji abonentów nazw domen i nawiązywania z nimi kontaktu. Zgodnie z treścią opinii, te istotne informacje powinny obejmować co najmniej nazwę abonenta, jego adres fizyczny i adres e-mail oraz numer telefonu. Jeżeli chodzi o zapewnienie dostępu do danych rejestracyjnych nazw domen uprawnionym podmiotom ubiegającym się o dostęp, opinia IMCO zawiera poprawkę zobowiązującą rejestry, rejestratorów i innych dostawców usług w zakresie rejestracji nazw domen do udzielania takim organom odpowiedzi w ciągu 72 godzin. Warto zauważyć, że poprawki zaproponowane przez IMCO odzwierciedlają takie samo podejście jak w przypadku ITRE.

A jak projekt dyrektywy NIS 2 komentuje CENTR (*Council of Europen National Top-Level Domain Registries*)?

CENTR podkreśla, że chociaż utrzymywanie bazy danych rejestracyjnych jest częścią obowiązków rejestrów ccTLD, WHOIS nie jest tym, co stanowi system nazw domen (DNS). Stwierdzenie dotyczące związku między dokładnymi i kompletnymi danymi rejestracyjnymi a bezpieczeństwem, stabilnością i odpornością DNS w art. 23 projektu dyrektywy NIS 2 jest, w opinii CENTR, błędne i nie odzwierciedla rzeczywistości cyberzagrożeń wymierzonych w infrastrukturę DNS. Według CENTR, art. 23 ust. 2 powinien zostać zmieniony w celu

uwzględnienia istotnych informacji umożliwiających identyfikację i kontakt z abonentami nazw domen oraz ich administratorami w ramach TLD. Według CENTR, takie informacje powinny ograniczać się do ściśle niezbędnych i właściwych w ramach odpowiedniej podstawy prawnej dla przetwarzania danych, przewidzianej w prawie EU lub prawie Państwa Członkowskiego. Mając na uwadze postanowienia art. 5 GDPR, art. 23 NIS 2 powinien, zgodnie z opinią CENTR, zawierać wyraźne wskazanie celu, w jakim dane dotyczące rejestracji nazw domen są przetwarzane przez rejestry TLD i podmioty świadczące usługi rejestracji nazw domen. W odniesieniu zaś do ust. 5 omawianego artykułu, CENTR podziela pogląd Komisji LIBE i IMCO i rekomenduje, aby lista uprawnionych podmiotów ubiegających się o dostęp była ograniczona do właściwych organów krajowych, w tym krajowych organów ścigania, pod warunkiem, że dostęp do danych rejestracyjnych udzielany będzie na podstawie odpowiedniej podstawy prawnej, która spełnia warunki określone w unijnych przepisach ramowych dotyczących ochrony danych.