Ida Jóźwiak[1]

ODPOWIEDZIALNOŚĆ DOSTAWCÓW USŁUG ZAUFANIA – WYBRANE ASPEKTY

STRESZCZENIE

Uregulowanie na poziomie Unii Europejskiej usług zaufania i środków identyfikacji elektronicznej stanowi odpowiedź na rosnące zapotrzebowanie w zakresie uregulowania kwestii m.in. potwierdzania tożsamości strony dokonującej czynności prawnej drogą elektroniczną i czasu dokonania czynności czy zapewnienia integralności treści składanych oświadczeń woli. Jednakże w dobie szybkiego postępu technologicznego i towarzyszącego mu rosnącego zagrożenia cyberprzestępczością nie jest możliwe pełne zagwarantowanie bezpieczeństwa dokonywania czynności prawnych drogą elektroniczną. Jako że do korzystania z usług elektronicznych niezbędne jest użycie odpowiedniego oprogramowania, do którego w sposób zdalny może mieć dostęp dostawca lub osoba nieuprawniona dokonująca ataku hakerskiego, w konsekwencji rodzi się pytanie o odpowiedzialność dostawców oprogramowania oraz sprzętu umożliwiającego korzystanie z usług zaufania za ich bezpieczeństwo, czyli odpowiedzialność dostawców usług zaufania. Celem artykułu jest przedstawienie wybranych, kluczowych z punktu widzenia bezpieczeństwa użytkowników i odbiorców usług zaufania aspektów tego zagadnienia.

SŁOWA KLUCZOWE

Usługi zaufania, internet, podpis elektroniczny, dokument elektroniczny

[1] Wydział Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie.

WPROWADZENIE

Stosowanie usług zaufania, czyli usług elektronicznych polegających na tworzeniu, weryfikacji, walidacji i konserwacji podpisów elektronicznych, pieczęci elektronicznych, elektronicznych znaczników czasu, rejestrowanych doręczeń elektronicznych, uwierzytelniania witryn internetowych za pomocą certyfikatów[2], ma na celu zasadniczo potwierdzenie tożsamości osoby podpisującej dokument elektroniczny w taki sposób, jak gdyby przy składaniu podpisu okazała odbiorcy oświadczenia swój dowód osobisty oraz zabezpieczenie dokumentu przed nieuprawnionymi modyfikacjami jego treści[3], ewentualnie również opatrzenie go datą pewną[4] czy potwierdzenie wysyłki i otrzymania danych przez zidentyfikowanego nadawcę i odbiorcę oraz dokładności daty i czasu tych zdarzeń[5]. Wspólną cechą zróżnicowanej rodzajowo kategorii usług zaufania jest ich ukierunkowanie na wyeliminowanie ryzykownej anonimowości uczestników czynności podejmowanych drogą elektroniczną i jednoczesne uwiarygodnienie ich działań poprzez m.in. uwierzytelnienie tożsamości strony dokonującej czynności[6], zapewnienie integralności (niezmienności) treści składanych oświadczeń woli[7], potwierdzenie czasu dokonania czynności[8].

Jednakże w dobie szybkiego postępu technologicznego i towarzyszącego mu rosnącego zagrożenia cyberprzestępczością nie jest możliwe pełne zagwarantowanie bezpieczeństwa dokonywania czynności prawnych drogą elektroniczną, podobnie jak tradycyjny obrót z wykorzystaniem własnoręcznie sygnowanych dokumentów nie jest całkowicie wolny od ryzyk takich jak fałszerstwo podpisu, dopiski, zagubienie czy zniszczenie dokumentu. Jako że do korzystania z usług elektronicznych niezbędne jest użycie odpowiedniego oprogramowania, do którego w sposób zdalny może mieć dostęp dostawca lub osoba nieuprawniona dokonująca ataku hakerskiego, w konsekwencji rodzi się pytanie o odpowiedzialność dostawców oprogramowania oraz sprzętu umożliwiającego korzystanie z usług zaufania za ich bezpieczeństwo, czyli odpowiedzialność dostawców usług zaufania. Celem niniejszego

[2] Art. 3 pkt 16 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.U. UE, L 257, 28 sierpnia 2014 r., s. 73–114), dalej: „rozporządzenie eIDAS".
[3] Por. art. 26 lit. d oraz art. 36 lit. d rozporządzenia eIDAS.
[4] W Polsce od 8 września 2016 r. kwalifikowany elektroniczny znacznik czasu wywołuje skutki daty pewnej (art. 81 § 2 pkt 3 KC).
[5] Por. art. 43 ust. 2 rozporządzenia eIDAS.
[6] Por. art. 26 lit. b oraz art. 36 lit. b rozporządzenia eIDAS.
[7] Por. art. 26 lit. d, art. 36 lit. d, art. 41 ust. 2, art. 43 ust. 2 rozporządzenia eIDAS.
[8] Por. art. 41 ust. 2, art. 43 ust. 2 rozporządzenia eIDAS.

artykułu będzie przedstawienie wybranych, kluczowych z punktu widzenia bezpieczeństwa użytkowników i odbiorców usług zaufania aspektów tego zagadnienia. Z uwagi na ograniczoną objętość tekstu, pojęcia i problemy bazowe, takie jak m.in. definicje poszczególnych usług zaufania, różnice między usługami kwalifikowanymi i niekwalifikowanymi, ich ramy i skutki prawne oraz praktyczne zastosowanie zostaną pominięte lub wspomniane jedynie zdawkowo.

Z uwagi na to, że jak dotąd tematyka odpowiedzialności dostawców zaufania pod rządami obecnie obowiązującego 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[9] (zwanego powszechnie rozporządzeniem eIDAS, jako akronim od anglojęzycznej nazwy *electronic IDentification, Authentication and trust Services*; dalej jako „rozporządzenie eIDAS"), nie doczekała się szerszego opracowania w doktrynie, a jej reżim jest skonstruowany w oparciu o doświadczenia związane z implementacją dyrektywy 1999/93/WE, w stosownym zakresie będę dokonywać porównań i korzystać z dorobku powstałego na gruncie poprzedniego stanu prawnego. Wskazana problematyka jak dotąd nie była przedmiotem wykładni Trybunału Sprawiedliwości Unii Europejskiej, ani na gruncie dyrektywy, ani rozporządzenia.

RAMY PRAWNE DZIAŁALNOŚCI DOSTAWCÓW USŁUG ZAUFANIA

Działalność dostawców usług zaufania stanowi przedmiot rozporządzenia eIDAS, a uzupełnieniem tej regulacji na terytorium Rzeczpospolitej Polski jest ustawa z dnia 5 września 2016 r. o *usługach zaufania* oraz identyfikacji elektronicznej[10] (dalej jako „ustawa o usługach zaufania", „u.u.z."). Rozporządzenie eIDAS zastąpiło dyrektywę 1999/93/WE Parlamentu Europejskiego i Rady z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych[11] (dalej jako „dyrektywa 1999/93/WE"), której celem było stworzenie wspólnotowych ram dla stosowania podpisu elektronicznego, umożliwiających swobodny, transgraniczny przepływ związanych z nim produktów i usług oraz zapewniających uznawanie jego skuteczności prawnej w podstawowym zakresie[12]. Jej zakres nie obejmował

[9] Dz.U. UE, L 257, 28 sierpnia 2014 r., s. 73–114.
[10] Dz.U. z 2019 r. poz. 162.
[11] Dz.U. UE L 013, 19 stycznia 2000 r., s. 12 – 20.
[12] Motyw 4 i 16 dyrektywy 1999/93/WE.

jednak wymogów formalnych dotyczących zawierania i skuteczności umów, które pozostały przedmiotem wewnętrznych regulacji Państw Członkowskich.

USŁUGI KWALIFIKOWANE I NIEKWALIFIKOWANE

Podpisy elektroniczne[13], pieczęci elektroniczne[14], elektroniczne znaczniki czasu[15], usługi rejestrowanego doręczenia elektronicznego[16] i certyfikaty uwierzytelniania witryn internetowych[17] mogą mieć postać niekwalifikowaną (zwykłą) lub kwalifikowaną, ponadto w przypadku podpisów elektronicznych i pieczęci elektronicznych wyróżnia się ich postacie zaawansowane, które można określić jako postacie pośrednie pomiędzy zwykłą a kwalifikowaną, ze względu na to, że spełniają wymagania techniczne określone dla postaci kwalifikowanej, natomiast w przeciwieństwie do niej nie uzyskały wymaganego przez rozporządzenie eIDAS kwalifikowanego certyfikatu. Kwalifikowana usługa zaufania definiowana jest jako usługa zaufania, która spełnia stosowne wymogi określone w rozporządzeniu[18]. Z usługami kwalifikowanymi powiązane są szczególne skutki i domniemania prawne[19].

ZASTOSOWANIE USŁUG ZAUFANIA

Zgodnie z założeniami europejskiego prawodawcy, usługi zaufania winny znaleźć szereg zastosowań zarówno w stosunkach prywatnoprawnych, jak i w kontaktach

[13] Podpis elektroniczny w rozumieniu art. 3 pkt 10 rozporządzenia eIDAS oznacza dane w postaci elektronicznej, które są dołączone lub logicznie powiązane z innymi danymi w postaci elektronicznej, i które użyte są przez podpisującego jako podpis.
[14] Pieczęć elektroniczna w rozumieniu art. 3 pkt 25 rozporządzenia eIDAS oznacza dane w postaci elektronicznej dodane do innych danych w postaci elektronicznej lub logicznie z nimi powiązane, aby zapewnić autentyczność pochodzenia oraz integralność powiązanych danych.
[15] Elektroniczny znacznik czasu w rozumieniu art. 3 pkt 33 rozporządzenia eIDAS oznacza dane w postaci elektronicznej, które wiążą inne dane w postaci elektronicznej z określonym czasem, stanowiąc dowód na to, że te inne dane istniały w danym czasie.
[16] Usługa rejestrowanego doręczenia elektronicznego w rozumieniu art. 3 pkt 36 rozporządzenia eIDAS oznacza usługę umożliwiającą przesłanie danych między stronami trzecimi drogą elektroniczną i zapewniającą dowody związane z posługiwaniem się przesyłanymi danymi, w tym dowód wysłania i otrzymania danych, oraz chroniącą przesyłane dane przed ryzykiem utraty, kradzieży, uszkodzenia lub jakiejkolwiek nieupoważnionej zmiany.
[17] Certyfikat uwierzytelniania witryn internetowych w rozumieniu art. 3 pkt 38 rozporządzenia eIDAS oznacza poświadczenie, które umożliwia uwierzytelnianie witryn internetowych i przyporządkowuje witrynę internetową do osoby fizycznej lub prawnej, której wydano certyfikat.
[18] Art. 3 pkt 17 rozporządzenia eIDAS.
[19] Por. art. 25 ust. 2-3, art. 35 ust. 2-3, art. 41 ust. 2-3, art. 43 ust. 2 rozporządzenia eIDAS.

z administracją publiczną, m.in. w bankowości elektronicznej, wystawianiu faktur, podpisywaniu umów, deklaracjach podatkowych, systemie opieki zdrowotnej, transakcjach *online*[20]. Charakter i ilość wymienianych danych, wymagany stopień bezpieczeństwa oraz skutki ewentualnego wycieku danych znacząco się różnią w każdym z przykładowo tylko wymienionych obszarów zastosowań, dlatego też poszczególne postaci usług zaufania (zwykła, kwalifikowana, zaawansowana) wywierają zróżnicowane skutki prawne, stosownie do oferowanego przez nie poziomu bezpieczeństwa. Najbardziej znane są usługi oparte na podpisie elektronicznym (tworzenie, weryfikacja, walidacja i konserwacja). Krajowa Izba Rozliczeniowa, jeden z kwalifikowanych polskich dostawców usług zaufania, jako przykłady zastosowania wydawanego przez siebie podpisu elektronicznego Szafir wymienia: deklaracje do ZUS w programie Płatnik, składanie sprawozdań finansowych do KRS, e-deklaracje do urzędów skarbowych, e-faktury, podpisywanie dokumentacji medycznej, uczestnictwo w przetargach i aukcjach elektronicznych, przesyłanie informacji do Generalnego Inspektora Informacji Finansowej i kontakty z urzędami[21]. Inny z dostawców, firma Asseco, dostawca podpisu elektronicznego Certum, uzupełnia tę listę m.in. o składanie wniosków o dotację do Polskiej Agencji Rozwoju Przedsiębiorczości, relacje biznesowe (B2B) oraz relacje biznesu z klientami (B2C), zastosowania w sądownictwie i więziennictwie – tj. do wzajemnej komunikacji sądów i służb penitencjarnych, sporządzania protokołów elektronicznych, przesyłania pism procesowych w elektronicznym postępowaniu upominawczym[22].

ZASADY ODPOWIEDZIALNOŚCI DOSTAWCÓW USŁUG ZAUFANIA

Podstawowym przepisem regulującym zasady odpowiedzialności dostawców usług zaufania jest art. 13 rozporządzenia eIDAS, który wyznacza podstawowe przesłanki odpowiedzialności, reguły rozkładu ciężaru dowodzenia oraz ustanawia możliwość ograniczenia zakresu odpowiedzialności dostawcy. Zarazem należy mieć na względzie, że regulacja zasad odpowiedzialności w rozporządzeniu nie jest kompletna i winna być stosowana

[20] *European Union Agency for Cybersecurity*, A digital Europe built on trust – ENISA supports relying parties and end users to implement the eIDAS Regulation, 29.06.2017 r., dostęp online: https://www.enisa.europa.eu/news/enisa-news/a-digital-europe-built-on-trust (data dostępu: 07.09.2019 r.)

[21] *Krajowa Izba Rozliczeniowa*, Certyfikaty kwalifikowane, dostęp online: http://www.elektronicznypodpis.pl/oferta/certyfikaty-kwalifikowane/ (data dostępu: 07.09.2019 r.)

[22] *Certum*, Podpis elektroniczny. Obszar zastosowania, dostęp online: https://www.certum.pl/pl/cert_oferta_epodpis_zastosowania/ (data dostępu: 07.09.2019 r.)

zgodnie z krajowymi przepisami dotyczącymi odpowiedzialności[23], w którego zakresie pozostaje m.in. określenie pojęcia i rozmiaru szkody czy zamiaru lub zaniedbania.

Zgodnie z art. 13 ust. 1 rozporządzenia, dostawcy usług zaufania są odpowiedzialni za szkody wyrządzone w sposób zamierzony lub z powodu zaniedbania osobie fizycznej lub prawnej w związku z niewypełnieniem obowiązków określonych w niniejszym rozporządzeniu. Przesłanki odpowiedzialności są następujące: zaistnienie szkody, zamiar wyrządzenia szkody lub zaniedbanie dostawcy usług zaufania oraz związek przyczynowy pomiędzy szkodą a niewypełnieniem obowiązków określonych w rozporządzeniu.

SZKODA

Na gruncie dyrektywy 1999/93/WE, podmiot świadczący usługi certyfikacyjne był odpowiedzialny jedynie za kilka rodzajów szkód określonych w art. 6 ust. 1 lit. a – c, tj.:

a) w zakresie zgodności wszelkich informacji zawartych w kwalifikowanym certyfikacie w momencie jego wydania oraz w zakresie kompletności danych przewidzianych dla certyfikatu kwalifikowanego;
b) w odniesieniu do zapewnienia, w momencie wydania certyfikatu podpisujący określony w certyfikacie kwalifikowanym posiadał dane służące do składania podpisu, które odpowiadają podanym lub określonym w certyfikacie danym służącym do weryfikacji podpisu;
c) w odniesieniu do zapewnienia, że w przypadkach, gdy podmiot świadczący usługi certyfikacyjne tworzy zarówno dane służące do składania podpisu, jak i dane służące do weryfikacji podpisu, mogą być one użyte w sposób dopełniający.

Oznaczało to, że szkody wynikające z innych przyczyn niż brak lub niepełna zgodność, kompletność, prawdziwość i komplementarność danych pozostały poza zakresem normowania dyrektywy, i o ile nie zostały ujęte szerszymi regulacjami prawa krajowego (dyrektywa ustanawiała minimalny poziom ochrony wymagany we wszystkich państwach członkowskich), podlegałyby ogólnym regułom odpowiedzialności odszkodowawczej w danym państwie.

[23] Por. motyw 18 rozporządzenia eIDAS.

W rozporządzeniu eIDAS ustawodawca europejski zrezygnował z tworzenia listy sytuacji, w których dostawca usług zaufania może ponieść odpowiedzialność odszkodowawczą, ustanowił natomiast kryterium powiązania szkody z niewypełnieniem obowiązków określonych w rozporządzeniu. Tytułem przykładu można wskazać kilka rodzajów szkód, jakie mogą powstać w związku z naruszeniem bezpieczeństwa lub utratą integralności usług zaufania: ujawnienie lub przechwycenie przez osobę nieuprawnioną poufnej korespondencji lub dokumentów, wyciek danych osobowych, w tym tzw. danych wrażliwych, modyfikacja treści dokumentów, oświadczeń woli (utrata integralności dokumentu), złożenie fałszywych oświadczeń woli, fałszywych podpisów pod oświadczeniami woli, przejęcie danych do logowania do różnych witryn internetowych, w tym do usług administracji publicznej świadczonych drogą elektroniczną, wyłudzenia pieniędzy, szantaże.

Oczywiście, wyżej wymienione sytuacje mogą skutkować powstaniem dalszych szkód. Jeżeli ujawniona zostałaby treść poufnego dokumentu zawierającego informacje objęte tajemnicą przedsiębiorstwa działającego na dużą skalę, jego straty związane z opublikowaniem tej informacji mogłyby być liczone w milionach euro. Wiele zależy od rodzaju danej usługi, jej zastosowania, rodzaju i skali naruszenia, szybkości reakcji dostawcy usług zaufania i innych. Określenie, na czym polega szkoda, jej rozmiaru i należnego odszkodowania, w szczególności czy powinno ono obejmować jedynie stratę rzeczywistą (*damnum emergens*) czy również utracone korzyści (*lucrum cessans*) będzie każdorazowo dokonywane przez właściwy sąd krajowy, według przyjętych w danym porządku prawnym dyrektyw interpretacyjnych.

ZWIĄZEK PRZYCZYNOWY POMIĘDZY SZKODĄ A NIEWYPEŁNIENIEM OBOWIĄZKÓW OKREŚLONYCH W ROZPORZĄDZENIU

Jedną z przesłanek odpowiedzialności dostawców usług zaufania, zarówno kwalifikowanych, jak i niekwalifikowanych, jest związek przyczynowy pomiędzy szkodą a niewypełnieniem obowiązków określonych w rozporządzeniu eIDAS. Tym samym, należyta realizacja obowiązków, nad którą czuwa sieć europejskich organów nadzoru, zwalnia dostawcę usług zaufania od odpowiedzialności za szkodę.

Zakres obowiązków dotyczących świadczenia usług zaufania jest odmienny dla dostawców niekwalifikowanych i kwalifikowanych, co jest w pełni uzasadnione odmiennością skutków prawnych poszczególnych rodzajów usług. Część wymogów określona

w rozporządzeniu eIDAS odnosi się do dostawców kwalifikowanych oraz niekwalifikowanych (art. 15, art. 19), część jedynie do kwalifikowanych (art. 20, art. 24).

Obowiązkami wspólnymi dla kwalifikowanych i niekwalifikowanych dostawców usług zaufania są:

1) Przyjęcie odpowiednich środków technicznych i organizacyjnych w celu zarządzania ryzykiem, na jakie narażone jest bezpieczeństwo świadczonych przez nich usług zaufania,

2) Zapewnienie poziomu bezpieczeństwa współmiernego z poziomem ryzyka, z uwzględnieniem najnowszych osiągnięć w dziedzinie technologii,

3) Podjęcie środków zapobiegających incydentom związanym z bezpieczeństwem lub minimalizujących ich wpływ oraz informowanie zainteresowanych stron o negatywnych skutkach wszelkich incydentów związanych z bezpieczeństwem,

4) Zawiadomienie organu nadzoru i innych właściwych podmiotów, takie jak właściwy krajowy organ ds. bezpieczeństwa informacji lub organ ochrony danych o wszelkich przypadkach naruszenia bezpieczeństwa lub utraty integralności oraz zawiadomienie osoby, na której rzecz była świadczona usługa zaufania o naruszeniu bezpieczeństwa lub utracie integralności, jeżeli występuje prawdopodobieństwo, że zdarzenie wpłynie na nią niekorzystnie,

5) W miarę możliwości, udostępnienie osobom niepełnosprawnym świadczonych usług zaufania oraz produktów przeznaczonych dla użytkownika końcowego stosowanych do świadczenia tych usług.

Kwalifikowani dostawcy usług zaufania są ponadto zobowiązani do:

1) Weryfikacji tożsamości i wszelkich specjalnych atrybutów przy wydawaniu kwalifikowanego certyfikatu dla usługi zaufania,

2) Informowania organu nadzoru o wszelkich zmianach w świadczeniu kwalifikowanych usług zaufania oraz o zamiarze zaprzestania działalności,

3) Zatrudniania pracowników lub podwykonawców dysponujących niezbędną wiedzą fachową, wiarygodnością, doświadczeniem, kwalifikacjami, którzy przeszli

odpowiednie szkolenia oraz stosują procedury administracyjne i zarządcze odpowiadające europejskim lub międzynarodowym standardom,

4) Utrzymywania dostatecznych zasobów finansowych lub posiadania ubezpieczenia od odpowiedzialności,

5) Informowania w jasny i szczegółowy sposób o dokładnych warunkach korzystania z usługi zaufania, w tym o wszelkich ograniczeniach,

6) Używania wiarygodnych systemów i produktów, chronionych przed modyfikacją i zapewniających techniczne bezpieczeństwo i wiarygodność obsługiwanych procesów,

7) Używania wiarygodnych systemów do przechowywania danych w sprawdzalnej postaci,

8) Podejmowania odpowiednich środków zapobiegających fałszowaniu i kradzieży danych,

9) Rejestrowania i udostępniania przez odpowiedni okres, w tym po zaprzestaniu działalności, wszelkich odpowiednich informacji dotyczących danych wydanych i otrzymywanych przez kwalifikowanego dostawcę, w szczególności do celów przedstawiania dowodów w postępowaniach sądowych i do zapewnienia ciągłości usług,

10) Posiadania aktualnego planu zakończenia działalności,

11) Zapewnienia zgodnego z prawem przetwarzania danych osobowych,

12) Tworzenia i aktualizacji bazy danych dotyczącej certyfikatów,

13) Rejestracji unieważnienia certyfikatu i publikacji informacji na ten temat w odpowiednim czasie, nie dłużej niż w ciągu 24 godzin od otrzymania wniosku,

14) Dostarczania w każdym momencie każdej stronie ufającej[24] informacji o statusie ważności lub unieważnienia kwalifikowanych certyfikatów w sposób automatyczny, wiarygodny, nieodpłatny i wydajny,

15) Poddania się audytowi przeprowadzanemu przez jednostkę oceniającą zgodność co najmniej raz na 24 miesiące, a także przeprowadzonemu przez organ nadzoru lub działającą na jego zlecenie jednostkę oceniającą zgodność – w dowolnym momencie.

Wymienione wyżej obowiązki są komplementarne, ich zakresy częściowo się ze sobą pokrywają, ale również uzupełniają, tworząc zbiór zasad bezpieczeństwa w działalności dostawców usług zaufania. Ich prawidłowe stosowanie skutkuje minimalizacją ryzyka wystąpienia szkody i ograniczeniem rozmiaru szkody w wypadku materializacji tego ryzyka. Niektóre z nich zostaną omówione poniżej, ze szczególnym uwzględnieniem potencjalnych skutków ich niewykonania lub nienależytego wykonania.

ZAPOBIEGANIE INCYDENTOM BEZPIECZEŃSTWA ORAZ INFORMOWANIE ZAINTERESOWANYCH STRON O ICH NEGATYWNYCH SKUTKACH

W art. 19 ust. 1 rozporządzenia eIDAS ustanowiono względem dostawców usług zaufania nakaz podjęcia odpowiednich środków technicznych i organizacyjnych w celu zarządzania ryzykiem, w szczególności poprzez podjęcie środków zapobiegających incydentom związanym z bezpieczeństwem lub minimalizujących ich wpływ. Incydent bezpieczeństwa definiuje się jako zdarzenie lub ciąg zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia procesów biznesowych o istotnym znaczeniu dla organizacji albo ujawnienia informacji posiadających dużą wartość dla organizacji lub chronionych z mocy prawa[25]. Przykładami incydentów bezpieczeństwa są: naruszenie poufności (ujawnienie

[24] Strona ufająca w rozumieniu art. 3 pkt 6 rozporządzenia eIDAS to osoba fizyczna lub prawna polegająca na identyfikacji elektronicznej lub usłudze zaufania. „Poleganie" oznacza, że taka osoba sprawdziła certyfikat związany z usługą zaufania (np. w następstwie otrzymania dokumentu elektronicznego opatrzonego podpisem elektronicznym, pieczęcią elektroniczną lub elektronicznym znacznikiem czasu) i upewniwszy się, iż jest on ważny, zaufała treści otrzymanego dokumentu lub witryny internetowej zabezpieczonej certyfikatem uwierzytelniania witryn internetowych. Strona ufająca nie musi być aktywnym użytkownikiem usług zaufania. Przeciwnie, wiele osób uzyskuje przymiot strony ufającej nie będąc tego świadomymi, chociażby otwierając akty prawne lub inne dokumenty urzędowe w wersji elektronicznej na stronach internetowych Biuletynu Informacji Publicznej.

[25] Definicja wskazana w normie PN-ISO/IEC 27000:2017-06.

niepowołanym osobom), integralności (uszkodzenie, zniszczenie), dostępności (uniemożliwienie dostępu), szkodliwe oprogramowanie, nieautoryzowany dostęp do systemu lub jego części, wyłudzenia haseł, kradzież lub zniszczenie urządzeń informatycznych oraz nośników danych[26]. To właśnie incydenty bezpieczeństwa będą najczęściej bezpośrednimi źródłami szkód powstałych u użytkowników usług zaufania, takich jak: naruszenie tajemnicy korespondencji, utrata środków pieniężnych (na skutek np. przechwycenia danych do logowania do systemu bankowości elektronicznej), zaistnienie zobowiązań i odpowiedzialności kontraktowej (w przypadku wykradzenia danych w celu złożenia stosownych oświadczeń woli do zawarcia umowy), złożenie niezgodnych z prawdą oświadczeń w stosunkach z administracją publiczną (np. złożenie nieprawdziwej deklaracji podatkowej w przypadku wykorzystania danych do składania podpisu elektronicznego) itd. Z tego względu, wszechstronne zabezpieczenie systemów i sieci teleinformatycznych stanowi kluczowy element działalności dostawców usług zaufania.

Dostawca usług zaufania jest zobowiązany do poinformowania zainteresowanych stron o negatywnych skutkach wszelkich incydentów związanych z bezpieczeństwem. Zainteresowaną stroną może być zarówno użytkownik usług zaufania, jak i każdy podmiot, który poniósł lub może ponieść szkodę związaną z incydentem, np. na skutek złożenia fałszywego oświadczenia woli z wykorzystaniem danych użytkownika. Poinformowanie strony ma na celu umożliwienie jej podjęcia czynności, które ograniczą lub wyeliminują dalsze szkody, poprzez chociażby zmianę haseł dostępowych czy odwołanie oświadczeń woli, które zostały złożone z wykorzystaniem jej danych.

ZAWIADAMIANIE WŁAŚCIWYCH ORGANÓW ORAZ OSÓB KORZYSTAJĄCYCH Z USŁUG ZAUFANIA

Zgodnie z art. 19 ust. 2 rozporządzenia eIDAS, kwalifikowani i niekwalifikowani dostawcy usług zaufania są zobowiązani do zawiadomienia organu nadzoru i innych właściwych podmiotów, takie jak właściwy krajowy organ ds. bezpieczeństwa informacji (w Polsce – minister właściwy do spraw informatyzacji) lub organ ochrony danych (w Polsce – Prezes Urzędu Ochrony Danych Osobowych) o wszelkich przypadkach naruszenia

[26] *D. Łydziński*, Procedury zarządzania incydentami bezpieczeństwa, IT Professional, 2 września 2016 r., dostęp: http://www.it-professional.pl/temat-numeru/artykul,6780,procedury-zarzadzania-incydentami-bezpieczenstwa.html (data dostępu: 10.09.2019 r.).

bezpieczeństwa lub utraty integralności, które mają znaczący wpływ na usługę lub przetwarzane w jej ramach dane osobowe. Zawiadomienie organów winno nastąpić bez zbędnej zwłoki, a w każdym razie nie później niż 24 godziny od otrzymania informacji o wystąpieniu zdarzenia. Obowiązek informacyjny winien być ponadto niezwłocznie zrealizowany względem osoby fizycznej lub prawnej na której rzecz była świadczona usługa zaufania, jeżeli występuje prawdopodobieństwo, że zdarzenie wpłynie na nią niekorzystnie. Celem zawiadomień jest zmniejszenie skali i rozmiaru szkód poprzez wydanie ostrzeżeń i zaleceń, a w poważniejszych przypadkach poprzez zawieszenie lub unieważnienie certyfikatów. Tym samym, szybkie wykrycie i zgłoszenie zaistniałego incydentu bezpieczeństwa ma zasadnicze znacznie dla rozmiaru odpowiedzialności odszkodowawczej.

Pewnych trudności może nastręczać wykładnia nieostrych pojęć „znaczącego wpływu" i „prawdopodobieństwa niekorzystnego wpływu na osobę". Wydaje się, że przy ocenie rozmiaru naruszenia i prawdopodobieństwa negatywnego oddziaływania należy brać pod uwagę przede wszystkim ustalenia dokonane w ramach analizy ryzyka, istotność naruszenia dla ciągłości świadczenia usług i ich integralności, rodzaj świadczonej usługi, ilość osób dotkniętych naruszeniem oraz potrzebę zastosowania środków nadzorczych przez właściwy organ, w szczególności zawieszenie lub unieważnienie certyfikatów. W porównaniu z obowiązkiem informowania zainteresowanych stron o negatywnych skutkach wszelkich incydentów bezpieczeństwa (art. 19 ust. 1 rozporządzenia eIDAS), obejmującym swoim zakresem nawet drobne zdarzenia, które nie wywołały żadnych szkód, obowiązek informowania o naruszeniach bezpieczeństwa i utracie bezpieczeństwa mających znaczący wpływ na usługę lub przetwarzane w jej ramach dane osobowe dotyczy poważniejszych sytuacji, raczej o charakterze systemowym niż jednostkowym.

W tym kontekście warto przytoczyć jeden z najbardziej znanych przykładów incydentów bezpieczeństwa, który doprowadził ostatecznie do upadłości holenderskiej firmy DigiNotar, wystawiającej certyfikaty w imieniu własnym oraz jako pośrednik w wydawaniu rządowych certyfikatów, które umożliwiały elektroniczny dostęp do usług administracji publicznej. W 2009 r. w protokole SSL służącym do bezpiecznej transmisji zaszyfrowanych danych i wykorzystywanym często w logowaniu do systemów bankowości elektronicznej czy poczty elektronicznej (użytkownik sieci Internet może łatwo zweryfikować, czy dana strona jest zabezpieczona protokołem – adres witryny w takim wypadku jest poprzedzony oznaczeniem https://, a dodatkowo wyświetla się znak kłódki), wykryto lukę, która umożliwiała dokonanie ataku hakerskiego znanego jako *Man in the Middle* („człowiek pośrodku"),

polegającego na uzyskaniu do informacji przesyłanych pomiędzy nieświadomymi tego faktu stronami korespondencji. W związku z tym, wydano rekomendację korzystania ze zaktualizowanych wersji protokołu i opublikowano informację o potencjalnie największym zagrożeniu związanym z użyciem protokołu, tj. włamaniu na serwer głównego centrum certyfikacyjnego i uzyskaniu dostępu do danych, dzięki którym możliwe jest generowanie podrabianych certyfikatów, akceptowanych przez przeglądarki internetowe jako prawdziwe. W ciągu kilku tygodni wygenerowano ponad pięćset fałszywych certyfikatów, w tym podmiotów takich jak CIA, Mossad, Google, Facebook, Twitter, Microsoft, Skype, a cyberprzestępcy uzyskali dostęp do treści poufnych rozmów i informacji. Choć Diginotar uzyskała informację o ataku 19.07.2011 r., przyznała się do niego dopiero z końcem sierpnia 2011 r., kiedy operatorzy popularnych przeglądarek internetowej zaczęli usuwać certyfikaty wystawiane przez DigiNotar z list zaufanych certyfikatów. 3.09.2011 r. wydano decyzję o unieważnieniu rządowych certyfikatów wystawionych przez firmę, co spowodowało utratę możliwości korzystania z usług administracji *online* przez wielu obywateli holenderskich. W wyniku przeprowadzonego dochodzenia ujawniono, że spółka nie posiadała ochrony antywirusowej na publicznym serwerze, stosowane przez nią oprogramowanie nie było aktualizowane, a system prewencyjny nie zablokował ataku z zewnątrz, w wyniku czego cyberprzestępcy złamali hasło administratora, uzyskując nieograniczony dostęp do wszystkich powiązanych serwerów. Nie udało się wyliczyć, ile osób poniosło szkody w związku z naruszeniem tajemnicy korespondencji, uzyskaniem przez hakerów dostępu do danych do logowania do wielu systemów czy utratą możliwości korzystania z usług administracji elektronicznej, jednakże mając na uwadze globalny zasięg oraz szczególną wrażliwość danych będących w posiadaniu części wyżej wskazanych podmiotów, których certyfikaty zostały sfałszowane, a także trwającą przez ponad miesiąc czasu bierność firmy DigiNotar w reakcji na zdarzenie, potencjalne szkody są trudne do przeszacowania[27].

Historia DigiNotar stanowi ilustrację wykorzystania niewystarczających, słabych i przestarzałych środków zabezpieczających, nieskutecznych mechanizmów wykrywania incydentów bezpieczeństwa i jednocześnie braku odpowiedniej reakcji usługodawcy na zaistniałe zagrożenie dla bezpieczeństwa, co ostatecznie doprowadziło do całkowitej utraty

[27] Opracowano na podstawie: *M. Marucha-Jaworska*, Podpisy elektroniczne, biometria, identyfikacja elektroniczna. Elektroniczny obrót prawny w społeczeństwie cyfrowym, Warszawa 2015, s. 147-148 oraz *European Union Agency for Network and Information Security*, Mitigating the impact of security incidents. Guidelines for trust service providers – part 3, wersja 1.0, grudzień 2013 r., dostęp online: https://www.enisa.europa.eu/publications/tsp3-incidents/ at_download/fullReport (data dostępu: 08.09.2019 r.), s. 23.

reputacji i konieczności ogłoszenia upadłości. Surowa sankcja zastosowana przez rząd holenderski – unieważnienie certyfikatów – odzwierciedla powagę naruszeń. Warto przy okazji zwrócić uwagę, że rozporządzenie eIDAS ustanawia sieć współpracy między organami nadzoru[28] (w Polsce tę funkcję pełni minister właściwy ds. informatyzacji), a jedną z form współpracy jest wymiana informacji miedzy organami nadzoru z państw dotkniętych naruszeniem bezpieczeństwa lub utratą integralności[29]. O zdarzeniu o charakterze transgranicznym organ nadzoru powinien ponadto zawiadomić ENISA[30] (Agencję Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji). Dodatkowo, jeżeli zawiadomiony organ nadzoru uzna, że ujawnienie naruszenia bezpieczeństwa lub utraty integralności leży w interesie publicznym, podaje taką informację do wiadomości publicznej lub nakazuje dostawcy, aby to uczynił[31].

Na mocy art. 46 pkt 8 w zw. z art. 47 ust. 2 pkt 1 ustawy o usługach zaufania, zaniedbanie wskazanych obowiązków informacyjnych przez kwalifikowanego dostawcę usług zaufania mającego siedzibę lub oddział na terytorium Rzeczpospolitej Polskiej może skutkować nałożeniem na niego kary pieniężnej w wysokości do 50 tysięcy złotych. Ograniczenie zakresu podmiotowego sankcji karnej w polskiej ustawie o usługach zaufania jest niezrozumiałe w obliczu faktu, że rozporządzenie europejskie nakłada obowiązek informacyjny zarówno na dostawców kwalifikowanych, jak i niekwalifikowanych, a trudno byłoby znaleźć argumenty na poparcie tezy, że przypadki poważnych incydentów bezpieczeństwa u tych drugich nie muszą być zgłaszane organom nadzoru, skoro również z usługami niekwalifikowanymi usługi wiąże się skutek prawnoprocesowy w postaci zakazu dyskryminacji (zakaz odmawiania skutku prawnego usłudze zaufania lub dokumentowi elektronicznemu ani ich dopuszczalności jako dowodu w postępowaniu sądowym wyłącznie z uwagi na ich elektroniczną postać lub niespełnienie wymagań formy kwalifikowanej). Argumentem na rzecz nieobejmowania niekwalifikowanych dostawców sankcją za niezrealizowanie obowiązków informacyjnych nie powinien być w szczególności ograniczony i następczy charakter działań nadzorczych w stosunku do dostawców niekwalifikowanych, skoro nadrzędnym celem objęcia systemem nadzoru wszystkich

[28] Por. motyw 42, art. 17 ust. 4 lit. a, art. 18 rozporządzenia eIDAS.
[29] Por. art. 17 ust. 4 lit. c, art. 19 ust. 2 rozporządzenia eIDAS.
[30] Art. 19 ust. 2 ak. 3 rozporządzenia eIDAS.
[31] Art. 19 ust. 2 ak. 4 rozporządzenia eIDAS.

dostawców usług zaufania winna być ochrona użytkowników i funkcjonowanie rynku wewnętrznego[32].

PRZECIWDZIAŁANIE FAŁSZOWANIU I KRADZIEŻY DANYCH

Wiarygodność założenia, że podpis elektroniczny (lub pieczęć elektroniczna) zostały złożone przez osobę uprawnioną, zależy z jednej strony od prawdziwości danych zawartych w certyfikacie na etapie jego wydawania, zaś z drugiej od skuteczności zabezpieczeń chroniących przed posłużeniem się certyfikatem przez nieuprawnionego. Z technicznego punktu widzenia, zabezpieczenie opiera się na algorytmach kryptograficznych asymetrycznych (tj. funkcjach matematycznych), charakteryzujących się tym, że dane łatwo jest zaszyfrować (łatwo jest obliczyć wynik danej funkcji), natomiast ich odkodowanie (matematycznie: odtworzenie wzoru funkcji na podstawie wyniku) jest na tyle skomplikowane, by odczytanie danych mogło nastąpić tylko z użyciem specjalnego klucza (który posiada osoba uprawniona) i było – z punktu widzenia kryptografii – niemożliwe[33] dla osób trzecich[34].

Sfałszowane lub skradzione mogą zostać jednak nie tylko dane osobowe zawarte w certyfikacie, ale również informacje (dane) zawarte w treści dokumentu elektronicznego, który został niedostatecznie zabezpieczony przez usługę zaufania. Sfałszowanie (nieuprawnione zmodyfikowanie w sposób, który nie jest łatwo rozpoznawalny) danych zawartych w dokumencie elektronicznym stanowi naruszenie jego integralności, której ochrona należy do istoty podpisu elektronicznego, pieczęci elektronicznej, elektronicznego znacznika czasu i rejestrowanego doręczenia elektronicznego. Natomiast kradzież danych w postaci elektronicznej różni się od zaboru materialnych ruchomości tym, że jej istotą jest zapoznanie się z tymi danymi przez osobę nieuprawnioną (dokonującą kradzieży) i ewentualne wykonanie ich nielegalnej kopii, do rzadkości należą przypadki jednoczesnego usunięcia danych z miejsca, do którego dostęp ma osoba uprawniona do posiadania danych (tj. uniemożliwienia dostępu do danych tej osobie). W konsekwencji, kradzież danych może pozostać niezauważona przez

[32] Motyw 36 rozporządzenia eIDAS.
[33] W kryptografii pojęcie niemożliwości nie jest pojęciem absolutnym, lecz oznacza, że czynność nie może być dokonana z wykorzystaniem znanych w danym momencie środków w akceptowalnym okresie czasu (za: *R. Wobst*, Kryptologia. Budowa i łamanie zabezpiecz*eń*, Warszawa 2002, s. 274.
[34] *M. Marucha-Jaworska,* op.cit., s. 106.

uprawnionego przez znaczny okres czasu – w Polsce przeciętnie rok[35]. Skradzione dane mogą być wykorzystane do różnego rodzaju celów, w tym szantaży i innego rodzaju wymuszeń. Przykładem kradzieży danych jest opisany powyżej atak typu *Man in the Middle.*

Krąg podmiotów, które potencjalnie mogą ponieść szkodę wynikającą z fałszerstwa lub kradzieży danych, jest bardzo szeroki.

Po pierwsze, poszkodowanym może być użytkownik usług zaufania, który poniósł szkodę w wyniku sfałszowania lub kradzieży danych zawartych w certyfikacie lub danych, którymi wymieniał się z innymi podmiotami, posługując się usługami zaufania. Szkoda użytkownika może polegać m.in. na samym zapoznaniu się przez podmiot nieuprawniony z danymi, ujawnieniu tych danych, roszczeniach podmiotów, których dane stały się przedmiotem fałszerstwa lub kradzieży, kierowanych względem użytkownika, stratach powstałych w wyniku czynności lub zaniechań, które nie miałyby miejsca, gdyby treść dokumentu elektronicznego nie została sfałszowana itd.

Po drugie, poszkodowanym może być strona ufająca, która działając w zaufaniu do danych zawartych w certyfikacie użytkownika usług zaufania lub w dokumencie zabezpieczonym usługą, dokonała pewnej czynności (np. zawarła umowę) lub zaniechała jej, podczas gdy postąpiłaby inaczej w wypadku, gdyby nie doszło do fałszerstwa danych.

Po trzecie, poszkodowanymi mogą być osoby, których dane osobowe zostały bez ich wiedzy i zgody zawarte w certyfikacie przez osobę fałszującą zawarte w nim dane – ich szkoda może polegać zarówno na samym bezprawnym wykorzystaniu ich danych osobowych, jak i kierowanych przeciwko nim roszczeniach stron ufających, działających w przeświadczeniu o istnieniu stosunku prawnego pomiędzy stroną ufającą a osobą, której dane zostały wykorzystane w certyfikacie.

Po czwarte, poszkodowanymi mogą być podmioty, których dotyczą sfałszowane lub skradzione dane, co może dotyczyć bardzo różnorodnych sytuacji, od sfałszowania (zmodyfikowania) informacji nt. tego podmiotu na stronie internetowej chronionej certyfikatem uwierzytelniania witryn internetowych, przez sfałszowanie lub kradzież danych dotyczących podmiotu zawartych w dokumencie przesyłanym pomiędzy stronami

[35] *PAP*, GIODO: Polak średnio po roku dowiaduje się o kradzieży tożsamości, 18.05.2015 r., https://www.pb.pl/giodo-polak-srednio-po-roku-dowiaduje-sie-o-kradziezy-tozsamosci-793371 (dostęp: 15.09.2019 r.).

korzystającymi z usług zaufania, po masową kradzież zbioru danych osobowych czy danych finansowych spółki i inne.

Rozmiar szkody doznanej przez poszkodowanego będzie zależał w znacznej mierze od tego, do czego zostaną wykorzystane dane skradzione lub jakie będą konsekwencje działania w oparciu o treść sfałszowanych danych.

PODSUMOWANIE

Podstawowe zasady odpowiedzialności dostawców usług zaufania wyznacza art. 13 rozporządzenia eIDAS, określający podstawowe przesłanki odpowiedzialności, reguły rozkładu ciężaru dowodzenia oraz ustanawia możliwość ograniczenia zakresu odpowiedzialności dostawcy. Jednocześnie należy mieć na względzie, iż regulacja zasad odpowiedzialności dostawców w rozporządzeniu nie jest kompletna, pozostawiając państwom członkowskim konieczność m.in. określenia pojęcia i rozmiaru szkody oraz współstosowania przepisów rozporządzenia wraz z krajowymi przepisami dotyczącymi odpowiedzialności. Dodatkowo, odpowiedzialność dostawców usług zaufania może być ograniczana z mocy stosownych postanowień prawa krajowego oraz polityk świadczenia usług tworzonych przez dostawców, co sprawia, że sąd rozpatrujący sprawę w tym przedmiocie będzie zmuszony rozstrzygać o odpowiedzialności odszkodowawczej dostawcy na podstawie norm prawa europejskiego, krajowego oraz postanowień umowy pomiędzy usługodawcą a użytkownikiem usług zaufania. Jak dotąd, ani polskie sądy, ani Trybunał Sprawiedliwości Unii Europejskiej nie miały okazji rozstrzygać o odpowiedzialności dostawców usług zaufania na gruncie rozporządzenia eIDAS (autorce nieznane są również żadne orzeczenia sądów państw członkowskich UE), trudno zatem o praktyczną ocenę przepisów w tym zakresie, jednakże wydaje się, że wskazana „wielopoziomowość" norm, do których sięgałby sąd, może przysporzyć niemałych trudności interpretacyjnych. W szczególności należy zwrócić uwagę na fakt, iż w zakresie normowania prawa krajowego pozostaje określenie pojęcia i rozmiaru szkody powstałej w wyniku niedopełnienia swoich obowiązków przez dostawcę, co potencjalnie może powodować znaczące różnice w orzecznictwie sądów różnych państw członkowskich w przedmiocie odpowiedzialności odszkodowawczej dostawców.

***

LIABILITY OF TRUST SERVICE PROVIDERS - SELECTED ASPECTS

The regulation of trust services and electronic identification means in the European Union responds to the growing demand for covering such issues as confirming the identity of the party performing the legal transaction by electronic means and the time of performing the action or ensuring the integrity of the content of submitted declarations of intent. Nonetheless, amidst rapid technological progress coupled with a growing threat of cybercrime, the security of electronic legal transactions may not be fully guaranteed. Whereas the use of electronic services requires the use of appropriate software, which can be remotely accessed by a supplier or unauthorized person carrying out a hacking attack, a question arises about the liability of providers software and hardware enabling the use of trust services for their security, that is the liability of trust service providers. This paper presents selected aspects of this issue, crucial from the point of view of security of users and recipients of trust services.

KEYWORDS

trust services, suppliers, eIDAS Regulation, electronic signature

BIBLIOGRAFIA

Marucha–Jaworska M., *Podpisy elektroniczne, biometria, identyfikacja elektroniczna. Elektroniczny obrót prawny w społeczeństwie cyfrowym*, Warszawa 2015.

PN-ISO/IEC 27000:2017-06 Technika informatyczna -- Techniki bezpieczeństwa -- Systemy zarządzania bezpieczeństwem informacji -- Przegląd i terminologia/

Wobst R., *Kryptologia. Budowa i łamanie zabezpieczeń*, Warszawa 2002.

Certum, *Podpis elektroniczny. Obszar zastosowania*, dostęp online: https://www.certum.pl/pl/cert_oferta_epodpis_zastosowania/ (data dostępu: 07.09.2019 r.)

European Union Agency for Cybersecurity, *A digital Europe built on trust – ENISA supports relying parties and end users to implement the eIDAS Regulation*, 29.06.2017 r., dostęp online:

https://www.enisa.europa.eu/news/enisa-news/a-digital-europe-built-on-trust (data dostępu: 07.09.2019 r.)

European Union Agency for Network and Information Security, *Mitigating the impact of security incidents. Guidelines for trust service providers – part 3*, wersja 1.0, grudzień 2013 r., dostęp online: https://www.enisa.europa.eu/publications/tsp3-incidents/at_download/fullReport (data dostępu: 08.09.2019 r.)

Krajowa Izba Rozliczeniowa, *Certyfikaty kwalifikowane*, dostęp online: http://www.elektronicznypodpis.pl/oferta/certyfikaty-kwalifikowane/ (data dostępu: 07.09.2019 r.)

Łydziński D., *Procedury zarządzania incydentami bezpieczeństwa, IT Professional*, 2 września 2016 r., dostęp: http://www.it-professional.pl/temat-numeru/artykul,6780, procedury-zarzadzania-incydentami-bezpieczenstwa.html (data dostępu: 10.09.2019 r.)

PAP, *GIODO: Polak średnio po roku dowiaduje się o kradzieży tożsamości*, 18.05.2015 r., https://www.pb.pl/giodo-polak-srednio-po-roku-dowiaduje-sie-o-kradziezy-tozsamosci-793371 (dostęp: 15.09.2019 r.).