MACIEJ GURTOWSKI
ORCID: 0000-0002-2990-9088

JAN WASZEWSKI
ORCID: 0000-0002-7370-3714

DOI: 10.4467/20801335PBW.21.021.14298

Niewidzialna infrastruktura Internetu – usługi chmurowe jako krytyczny element środowiska bezpieczeństwa. Przypadek Amazona

Na wstępie warto przeprowadzić pewien eksperyment myślowy: wyobraźmy sobie, że z powodu awarii, sabotażu lub celowych sankcji Polska zostaje pozbawiona możliwości korzystania z zasobów amerykańskich gigantów technologicznych z grupy GAFAM[1]. Jakie będą konsekwencje awarii i czy instytucje państwowe, podmioty prywatne oraz zwykli użytkownicy byliby w stanie w takiej sytuacji funkcjonować bez poważnych zakłóceń? Łatwo przewidzieć, że niemożność korzystania z chociażby samych systemów operacyjnych: Windows, Android czy MacOS/iOS miałaby katastrofalne następstwa. Mniej oczywiste, co nie znaczy, że mniej istotne, byłyby skutki zablokowania innych funkcjonalności, takich jak usługi chmurowe gigantów technologicznych. Właśnie temu mniej oczywistemu problemowi uzależnienia od usług chmurowych poświęcono niniejszy artykuł.

Na początku 2019 r. amerykańska dziennikarka Kashmir Hill w cyklu artykułów zatytułowanych *Żegnaj wielka piątko*[2] przedstawiła eksperyment, który przeprowadziła. Za pomocą informatycznych narzędzi zablokowała sobie dostęp do infrastruktury i usług kolejnych członków GAFAM. W pierwszym etapie zrezygnowała z produktów

[1] Akronim został stworzony z pierwszych liter nazw najważniejszych amerykańskich firm z branży nowych technologii, tj. Google, Amazon, Facebook, Apple i Microsoft. Inne określenie tej grupy to Big Tech.

[2] K. Hill, *Goodbye Big Five*, Gizmodo, 7 II 2019 r., https://gizmodo.com/c/goodbye-big-five [dostęp: 4 III 2021]. Tłumaczenia w artykule pochodzą od autorów (przyp. red.).

Amazona, jego usług streamingu filmów i seriali oraz ze sklepu internetowego. W kolejnym kroku odcięła się od wszystkich stron internetowych i aplikacji, które korzystają z usług chmurowych Amazona. Dość szybko okazało się, że wiele firm, również konkurencyjnych dla Amazona, opiera swoją działalność na jego infrastrukturze. W krótkim czasie dziennikarka zrozumiała, że: *Amazon jest głęboko zakorzeniony w jej życiu. Używa go wielokrotnie każdego dnia świadomie i nieświadomie. Nie jest w stanie bez niego normalnie funkcjonować*[3].

W niniejszym artykule autorzy przyjęli systemową koncepcję środowiska bezpieczeństwa[4]. Jest ona przeciwstawiana bardziej rozpowszechnionemu, intuicyjnemu podejściu do spraw bezpieczeństwa, w którym uwaga jest skupiana na jego bezpośrednich zagrożeniach. W przypadku bezpieczeństwa ograniczanie się do badania zagrożeń, bez uwzględniania towarzyszących im kontekstów, może prowadzić do błędów poznawczych. W podejściu systemowym właśnie konteksty stają się właściwym przedmiotem analizy. Zgodnie z przyjętym podejściem środowisko bezpieczeństwa ma naturę systemową, a zatem jego analiza powinna uwzględniać wiele czynników oraz dynamiczne interakcje między nimi. Jednym z najważniejszych jest technologia[5]. W analizie systemowej przyjmuje się, że środowisko bezpieczeństwa jest aktywnie, intencjonalnie i nieintencjonalnie kształtowane przez państwa i inne wpływowe podmioty. Autorzy artykułu skoncentrowali się na amerykańskich gigantach technologicznych.

Przedmiotem analizy jest jeden z głównych zasobów GAFAM, tj. usługi chmurowe, oraz aktualnie największy ich globalny dostawca – firma Amazon Web Services[6] (dalej: AWS), działająca od 2002 r. spółka zależna Amazona, która oferuje takie usługi od 2006 r. W czwartym kwartale 2020 r. miała ona w tym sektorze usług 32 proc. udziału w rynku światowym[7]. Druga w kolejności firma – Microsoft Azure dysponowała w tym samym czasie 20-procentowym udziałem w rynku, Google Cloud – 7-procentowym, a chiński Alibaba Cloud – 6-procentowym. Pozostałą część tego rynku kontrolowały drobniejsze podmioty. Można powiedzieć, że infrastruktura dostarczana przez Amazona i innych dostawców usług chmurowych w coraz większym stopniu

---

[3] K. Hill, *I Tried to Block Amazon From My Life. It Was Impossible*, Gizmodo, 22 I 2019 r., https://gizmodo.com/i-tried-to-block-amazon-from-my-life-it-was-impossible-1830565336 [dostęp: 24 III 2021].

[4] S. Tang, *A systemic theory of the security environment*, „Journal of Strategic Studies" 2004, nr 1, s. 1–3; por. G.H. Turbiville, W.W. Mendel, J.W. Kipp, *The Changing security environment*, „Military Review" 1997, nr 77, s. 5–10.

[5] S. Tang, *A systemic theory of the security environment*…, s. 2–3, 7; Centrum Doktryn i Szkolenia Sił Zbrojnych, *Analiza środowiska bezpieczeństwa w perspektywie 2035 r.*, Bydgoszcz 2020, https://cdissz.wp.mil.pl/pl/articlespublikacje_cdissz/analiza-srodowiska-bezpieczenstwa-w-perspektywie-2035-roku-pl/ [dostęp: 24 III 2021].

[6] Wyróżnienia w tekście pochodzą od autorów (przyp. red.).

[7] *Global cloud services market Q4 2020*, Canalys, 2 II 2021 r., https://www.canalys.com/newsroom/global-cloud-market-q4-2020 [dostęp: 5 III 2021].

pełni funkcję niewidzialnej infrastruktury Internetu[8]. Z usług chmurowych tej spółki korzysta tak wiele firm i instytucji, że awarie występujące u amerykańskiego giganta handlu internetowego były opisywane jako awarie całego Internetu[9]. Biorąc pod uwagę pozycję rynkową Amazona, autorzy artykułu podjęli decyzję, że w ramach studiów przypadków[10] zostaną przedstawione działania właśnie tej spółki. Wyzwania związane z usługami chmurowymi nie dotyczą jednak tylko AWS i innych członków GAFAM czy też firmy Alibaba Cloud.

W artykule zostają postawione dwa pytania badawcze:

1. W jaki sposób rozpowszechnienie się korzystania z usług chmurowych wpływa na globalne środowisko bezpieczeństwa?
2. Jakie zagrożenia stwarza zjawisko monopolizacji usług chmurowych?

W odpowiedzi na te pytania autorzy rozważą następujące hipotezy:

1. Rozpowszechnienie korzystania z usług chmurowych sprawia, że podmioty je oferujące zyskują narzędzia inwigilacji i potężnego, dyskrecjonalnego wpływu na swoich klientów (użytkowników) i relacje między nimi.
2. Monopolizacja usług chmurowych prowadzi do centralizacji struktury Internetu, tworząc nowe źródła podatności sieci na zakłócenia jej działania, związane z rosnącą zależnością coraz większej liczby użytkowników od coraz mniejszej liczby dostawców usług w chmurze.

W metodologii wykorzystanej w artykule studia przypadków odgrywają rolę uchwytnych empirycznie i przez to możliwych do uściślenia lub podważenia egzemplifikacji problemu przekształceń środowiska bezpieczeństwa, wynikających z rozpowszechnienia się korzystania z usług chmurowych.

Artykuł ma następującą strukturę. Na początku przedstawiono rozważania definicyjne porządkujące poruszane zagadnienia. W dalszej części tekstu odwołano się do literatury przedmiotu dotyczącej typowych sposobów analizowania zagrożeń związanych ze stosowaniem chmury obliczeniowej. Następnie zaprezentowano dwa krótkie

---

[8] M. Day, *Amazon Cloud Outage Hits Customers Including Roku, Adobe*, Bloomberg, 25 XI 2020 r., https://www.bloomberg.com/news/articles/2020-11-25/amazon-web-services-outage-hits-cloud-customers [dostęp: 7 XII 2020].

[9] J. Del Rey, *Amazon's massive AWS outage was caused by human error*, „Recode", 2 III 2017 r., https://www.vox.com/2017/3/2/14792636/amazon-aws-internetoutage-cause-human-error-incorrect-command [dostęp: 11 XII 2020]; K. Hill, *I Tried to Block Amazon…*

[10] Są to konkretnie instrumentalne studia przypadków (*instrumental case study*), które są jednym ze sposobów podejścia do analizy przypadku (wszystkie wyrazy i zwroty obcojęzyczne w artykule pochodzą z języka angielskiego, dlatego Redakcja nie podaje za każdym razem tej informacji – dop. red.). To podejście służy jak najbardziej wyrazistemu zilustrowaniu danego zjawiska, jego przyczyn i skutków. Sam przypadek odgrywa w nim rolę pomocniczą. Zob. R.E. Stake, *Jakościowe studium przypadku*, w: *Metody badań jakościowych*, N.K. Denzim, Y.S. Lincoln (red.), Warszawa 2009, t. 1, s. 627–629.
Punktem wyjścia dla studiów przypadków zawartych w niniejszym artykule były analizy prowadzone przez autorów w ramach ich pracy w Centrum Badań nad Bezpieczeństwem Akademii Sztuki Wojennej w Warszawie.

studia przypadków, które ilustrują zagrożenia związane z rozwojem usług chmurowych. W kolejnym kroku pokazano, że znaczenie takiej chmury dla środowiska bezpieczeństwa stale rośnie. Na podstawie m.in. ustaleń amerykańskiej parlamentarnej podkomisji antytrustowej wykazano, że głównych dostawców chmury trudno nazwać partnerami, co do których wiarygodności nie ma poważnych wątpliwości. Artykuł kończą wnioski, zawierające syntezę przeprowadzonych rozważań.

Czym jest i jak działa chmura? Najważniejsze pojęcia

W celu uporządkowania niniejszego wywodu warto przyjrzeć się najważniejszym pojęciom związanym z systemem usług chmurowych.

Koncepcję uruchomienia chmury obliczeniowej w jej współczesnym rozumieniu przypisuje się właśnie Amazonowi[11]. Około 2003 r. spółka uznała, że skoro posiada dużą liczbę komputerów połączonych w sieć, które np. nocą nie są w USA w pełni wykorzystywane, to można je zdalnie i odpłatnie udostępnić komuś z innych części świata. W 2006 r. powstał system łączący dostępne zdalnie komputery (w nomenklaturze AWS jest to usługa E2C), magazyny danych (usługa S3) oraz narzędzie do wynajmowania ludzi do realizowania zdalnie zadań, których obecnie nie można wykonać automatycznie (usługa *Mechanical Turk*)[12].

Zgodnie z ogólnie przyjętą definicją zaproponowaną przez amerykański Narodowy Instytut Standardów i Technologii (National Institute of Standards and Technology, NIST): (…) *chmura obliczeniowa* [*cloud computing*] *to model* [działania] *pozwalający na osiągalny wszędzie i na żądanie wygodny dostęp za pomocą sieci do podzielanej puli możliwych do skonfigurowania zasobów (np. sieci, serwerów, przestrzeni magazynowej, aplikacji i usług), które mogą być szybko dostarczane i uaktywniane z minimalnym wysiłkiem zarządczym lub niewielkim kontaktem z dostawcą*[13]. Innymi słowy, „chmura obliczeniowa" to dostępne zdalnie komputery, podłączone do nich dyski twarde i obecne na nich oprogramowanie, które klienci mogą łatwo wykorzystać do realizowania swoich potrzeb. Ich zaspokajanie jest skalowalne – można wynajmować aktualnie potrzebną ilość mocy obliczeniowej czy przestrzeni do magazynowania danych. Serwerownie lub centra danych, w których mieszczą się komputery wchodzące w skład chmury, mogą korzystać z efektu skali. Duża liczba znajdujących się w jednym miejscu komputerów

[11] Ryan Ko, Kim-Kwang Raymond Choo, *Cloud Security Ecosystem*, w: *The Cloud Security Ecosystem. Technical, Legal, Business and Management Issues*, Ryan Ko, Kim-Kwang Raymond Choo (red.), Waltham 2015, s. 1.

[12] Tamże, s. 2.

[13] P. Mell, T. Grance, *The NIST Definition of Cloud Computing*, wrzesień 2011 r., https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf [dostęp: 4 III 2021]. Również *Uchwała nr 97 Rady Ministrów z dnia 11 września 2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa"* (MP z 2019 r. poz. 862) wydaje się w części słownikowej korzystać z definicji NIST dotyczących chmury obliczeniowej i innych pojęć z nią związanych.

sprawia, że spadają np. koszty ich serwisowania i chłodzenia, energii elektrycznej oraz zwiększania lub zmniejszania zasobów dostępnych dla klientów wraz z ich rosnącymi lub malejącymi potrzebami.

Standardowo chmury dzieli się pod kątem tego, kto ma bezpośrednią kontrolę nad infrastrukturą i do jak daleko idącego *outsourcingu* usług informatycznych dochodzi. W dużym uproszczeniu podział opiera się więc na tym, kto ma fizyczny dostęp do serwerów i odpowiada za ich działanie. W wypadku chmury prywatnej kontrolę nad nią dzierżą firmy lub osoby fizyczne, które zbudowały dla siebie serwerownię czy centrum danych. Chmura społecznościowa znajduje się pod kontrolą użytkowników z różnych organizacji, które podzielają pewien cel, ideę lub zadania publiczne. Chmura publiczna oznacza infrastrukturę znajdującą się na serwerach dostawcy i dostępną praktycznie dla każdego, kto zakupi do niej dostęp. Chmura może być również hybrydowa, czyli łączyć różne cechy wcześniej wymienionych typów.

Przyjmuje się, że istnieją trzy główne modele realizowania usług chmurowych:

1) infrastruktura jako usługa (*Infrastructure as a Service*, IaaS),
2) platforma jako usługa (*Platform as a Service*, PaaS),
3) oprogramowanie jako usługa (*Software as a Service*, SaaS).

Kolejność wymienienia tych modeli jest zgodna z rosnącym zakresem kontroli powierzonej dostawcy nad oferowanymi rozwiązaniami. W wypadku IaaS chmura to tylko czysta infrastruktura, to znaczy dostępne zdalnie komputery. PaaS daje użytkownikowi kontrolę również nad swoimi aplikacjami i konfiguracją komputerów, ale już system operacyjny, narzędzia w niego wbudowane i obsługa języków programowania są dostarczane przez dostawcę usług chmurowych. Z kolei w modelu SaaS użytkownik korzysta z aplikacji działających w chmurze za pomocą interfejsu, takiego jak np. przeglądarka internetowa, i ma wpływ tylko na minimalną liczbę ustawień.

Obecnie zachodzą duże zmiany strukturalne w sposobach tworzenia oprogramowania[14]. Jedną z najważniejszych jest przejście z software'u działającego na urządzeniach użytkowników na usługi chmurowe. Dzięki tym usługom zaistniały i nabrały rozmachu opisane w artykule zjawiska, wskazywane w różnych analizach dotyczących IaaS, PaaS czy SaaS. Pojawiły się również m.in. usługi chmurowe w postaci analizy danych jako usługi (*Data as a Service*, DaaS), bezpieczeństwa jako usługi (*Security as a Service*, SECaaS[15]), platform kontenerowych[16] czy dostępnych zdalnie systemów

[14] S. Gürses, J. Van Hoboken, *Privacy After the Agile Turn*, w: *Cambridge Handbook of Consumer Privacy*, J. Polonetsky, O. Tene, E. Selinger (red.), Cambridge 2017, https://osf.io/preprints/socarxiv/9gy73/ lub https://osf.io/ufdvb/ [dostęp: 22 III 2021].

[15] B. Delamore, Ryan K.L. Ko, *Security as a service (SECaaS) – An overview*, w: *The Cloud Security Ecosystem. Technical, Legal, Business and Management Issues*, Ryan Ko, Kim-Kwang Raymond Choo (red.), Waltham 2015, s. 187–202.

[16] Są to zamknięte środowiska służące do uruchamiania aplikacji na różnych systemach operacyjnych. Jest to możliwe dzięki temu, że w „kontenerze" znajdują się wszystkie elementy potrzebne aplikacji do pracy (zob. np. *Co to jest kontener?*, https://azure.microsoft.com/pl-pl/overview/what-is-a-container/ [dostęp: 24 III 2021]).

sztucznej inteligencji[17]. Każdy z tych typów usług chmurowych ma niebagatelny wpływ na to, jak działa współczesny sprzęt komputerowy (hardware) oraz oprogramowanie, a tym samym na korzystające z nich podmioty (gospodarcze, publiczne). Podsumowując, zgodnie z aktualnymi konwencjami terminologicznymi chmura to nie tylko infrastruktura oraz programy (proces ich tworzenia, modyfikowania i wykorzystywania), lecz także analiza danych, *outsourcing* cyberbezpieczeństwa, wykrywanie wzorców i automatyzacja różnych działań za pomocą systemów sztucznej inteligencji (jako przykład można wskazać system JEDI opisany w dalszej części artykułu).

Innym ważnym pojęciem jest „*multicloud*", czyli bazowanie na zasobach wielu chmur, aby wykorzystać najbardziej użyteczne rozwiązania dostarczane przez różnych dostawców i nie uzależniać się od jednego z nich. *Multicloud* jest zagrożeniem modelu biznesowego dostawców usług chmurowych, którzy chcieliby kompleksowo zaspokajać potrzeby klientów i być za to opłacani. W takim modelu dąży się do uniknięcia sytuacji, w której klient może z łatwością zrezygnować z usług danego dostawcy lub z ich części.

Obowiązującym obecnie standardem dla publicznej chmury obliczeniowej jest zapewnianie klientom złożonych systemów usług, powiązanych ze sobą i wspierających się nawzajem. W opisanych poniżej studiach przypadków zostały przedstawione dwa typy znanych zagrożeń wynikających ze złożoności chmury. Po pierwsze, są to jej awarie (*outage*), które w połączeniu z możliwymi efektami kaskadowymi prowadzą do rozchwiania, a nawet załamania się części lub całości wspomnianego systemu[18]. Drugim znanym rodzajem zagrożenia jest uzależnienie się od usług stworzonych przez danego dostawcę (*vendor lock-in*)[19]. Ze względu na złożoność systemów poszczególnych dostawców utrudnione – a nawet niemożliwe – staje się sprawne odbudowanie funkcjonalności systemu klienta po zakończeniu przez niego współpracy z danym dostawcą chmury. Z tego powodu już na etapie planowania korzystania z chmury należy ustalić, czy będzie możliwe przejście do innego dostawcy usług chmurowych lub powrócenie do korzystania z własnych systemów[20].

Na poziomie ogólnych zasad działania rozwiązania chmurowe są stosunkowo proste. Korzystanie z nich wiąże się jednak z ryzykiem i wieloma zagrożeniami. W niniejszym artykule omówiono je na podstawie przeglądu literatury.

---

[17] Pod pojęciem „sztucznej inteligencji" jako usługi chmurowej należy rozumieć usługę zdalnej analizy danych w celu np. rozpoznawania obrazów (w tym identyfikowania ludzi na podstawie ich zdjęć czy odczytywania tablic rejestracyjnych), przekładanie wypowiadanych słów na tekst, udzielanie odpowiedzi przez bota na zadane mu pytania itp.

[18] Z pogłębioną, jednak pochodzącą sprzed pięciu lat, analizą przyczyn zakłóceń działania chmury można zapoznać się w: H.S. Gunawi i in., *Why Does the Cloud Stop Computing? Lessons from Hundreds of Service Outages*, w: *Proceedings of the Seventh ACM Symposium on Cloud Computing (SoCC '16)*, New York 2016, s. 1–16.

[19] T. Kemmericha, V. Agrawala, C. Momsen, *Secure migration to the cloud – In and out*, w: *The Cloud Security Ecosystem. Technical, Legal, Business and Management Issues*, Ryan Ko, Kim-Kwang Raymond Choo (red.), Waltham 2015, s. 205–230.

[20] Tamże, s. 214–215.

Analizy zagrożeń związanych z rozwiązaniami chmurowymi w literaturze przedmiotu

W 2009 r. Bruce Schneier, znany amerykański badacz zagadnień związanych z cyberbezpieczeństwem, zwrócił uwagę na bardzo ważny aspekt działania chmury obliczeniowej, jakim jest konieczność posiadania zaufania do dostawcy usług[21]. Ważne są cztery filary tego zaufania, tj. bezpieczeństwo, odporność, dostępność i trwałość działalności gospodarczej dostawcy. Pierwsze trzy z tych czynników dotyczą problemów wynikających z awarii i działań służących ograniczeniu ich odległych konsekwencji. Czwarty czynnik obejmuje zagadnienia związane z *vendor lock-in*, czyli wspomniane wyżej problemy wynikające z zakończenia współpracy z danym dostawcą – nie tylko z powodu zaprzestania przez niego działalności.

Trzy najczęściej cytowane artykuły naukowe na temat bezpieczeństwa chmur obliczeniowych pochodzą z lat 2009–2010[22]. Ich wspólnym elementem jest wskazanie, że korzystanie z rozwiązań chmurowych wiąże się z przyjęciem określonego ryzyka. Tymczasem można odnieść wrażenie, że chociaż coraz więcej poważnych przedsięwzięć w sieci opiera się na korzystaniu z chmury, to wiele podmiotów zdaje się to ryzyko ignorować.

Opublikowana w 2015 r. praca zbiorowa zatytułowana *Cloud Security Ecosystem* pokazuje, jak bardzo wielowymiarowy staje się problem uwzględnienia różnych aspektów bezpieczeństwa chmury obliczeniowej[23]. W 22 rozdziałach wspomnianej publikacji zagrożenia są analizowane z perspektywy m.in. technologii, prawa, zarządzania oraz działalności gospodarczej.

Rola gigantów internetowych, w tym spółek amerykańskich określanych jako GAFAM oraz chińskich, których pierwsze litery nazw łączą się w często używany akronim BATX (Baidu, Alibaba, Tencent, Xiaomi), jest we współczesnym świecie na tyle duża, że ich działalność analizuje się także z perspektywy pełnienia przez nie funkcji publicznych[24]. Cztery z dziewięciu wspomnianych spółek, tj. Amazon, Google,

---

[21] B. Schneier, *Cloud Computing*, Schneier on Security, 4 VI 2009 r., https://www.schneier.com/blog/archives/2009/06/cloud_computing.html [dostęp: 17 III 2021].

[22] Zgodnie z informacjami z wyszukiwarki Google Scholar. Wyszukiwana fraza to „cloud security". Stan na 23 III 2021 r. Wspomniane artykuły to: B.R. Kandukuri, R.V. Paturi, A. Rakshit, *Cloud Security Issues*, w: *Procedings of the 2009 IEEE International Conference on Services Computing*, Washington 2009, s. 517–520, https://ieeexplore.ieee.org/document/5283911 [dostęp: 23 III 2021]; S. Ramgovind, M.M. Eloff, E. Smith, *The Management of Security in Cloud Computing*, w: *2010 Information Security for South Africa (ISSA 2010)*, 2010 r., s. 1–7; M. Almorsy, J. Grundy, I. Müller, *An analysis of the cloud computing security problem*, w: *Proceedings of the APSEC 2010 Cloud Workshop*, Sydney 2010, s. 6. Te trzy artykuły miały odpowiednio 847, 584 i 497 cytowań.

[23] *The Cloud Security Ecosystem*…

[24] L. Taylor, *Public Actors Without Public Values: Legitimacy, Domination and the Regulation of the Technology Sector*, „Philosophy & Technology", 20 I 2021 r., https://link.springer.com/article/10.1007/s13347-020-00441-4 [dostęp: 22 III 2021]. Por. M. Gurtowski i J. Waszewski, *Wpływ działalności gigantów technologicznych na globalne środowisko bezpieczeństwa. Studium przypadku spółki Amazon*, „Kwartalnik Bellona" 2020, nr 3, s. 37–56.

Microsoft i Alibaba, są największymi globalnymi dostawcami usług chmurowych. Te z kolei w coraz większym stopniu są wykorzystywane także do realizowania funkcji publicznych, bardzo ważnych dla współczesnego globalnego środowiska bezpieczeństwa. Tym samym zakłócenia w ich działaniu są naruszeniem niewidzialnej, bo często pomijanej (pomimo ostrzeżeń oraz dobrych praktyk przywołanych w dalszej części artykułu), infrastruktury Internetu. Eksperci nie stawiają w sposób systemowy pytań o władzę, jaką dysponują firmy technologiczne, i o rolę, jaką chmura obliczeniowa odgrywa we współczesnej infrastrukturze krytycznej. Zdaniem autorów artykułu jest to poważna luka w literaturze przedmiotu.

Nie tylko badacze i analitycy, lecz także różne instytucje i urzędy na świecie zgodnie wskazują na wiele korzyści i zagrożeń związanych z korzystaniem z chmury obliczeniowej. Przykładowo, Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (European Union Agency for Cybersecurity, dalej: ENISA – akronim pochodzi od wcześniejszej nazwy Agencji – European Network and Information Security Agency, Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji) przygotowuje analizy oraz wyznacza standardy dotyczące usług chmurowych[25]. Warto zwrócić uwagę na opracowany przez nią dokument z grudnia 2012 r., w którym przeanalizowano korzyści i ryzyko związane z korzystaniem z tego rodzaju usług w kontekście bezpieczeństwa informacji[26]. Według wspomnianej agencji główne niebezpieczeństwa wiążą się m.in. z uzależnieniem od jednego dostawcy i brakiem możliwości przeprowadzania pełnego audytu ochrony danych wrażliwych. Inne zagrożenia wskazane w tym dokumencie w odpowiednich okolicznościach mogą wywołać awarie, a nawet efekty kaskadowe. W analizie poświęconej chmurze obliczeniowej jako infrastrukturze krytycznej ENISA przypomina również, że jest ona mieczem obosiecznym[27]. Z jednej strony najwięksi dostawcy dzięki rozproszeniu kosztów mogą oferować najlepsze i najnowocześniejsze środki zwiększające bezpieczeństwo i odporność, z drugiej jednak strony, (…) *jeśli pojawi się awaria lub włamanie, to konsekwencje również będą większe, wpływając jednocześnie na większą ilość danych, wiele organizacji i wielu obywateli*[28].

W styczniu 2020 r. amerykańska Agencja Bezpieczeństwa Narodowego (National Security Agency, dalej: NSA) opublikowała informacje na temat dobrych praktyk mających służyć minimalizowaniu zagrożeń związanych z korzystaniem z chmury

---

[25] European Union Agency for Cybersecurity, *Cloud and Big Data*, https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security [dostęp: 22 III 2021].

[26] European Network and Information Security Agency, *Cloud Computing. Benefits, risks and recommendations for information security*, rev. B z grudnia 2012 r., https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security [dostęp: 22 III 2021].

[27] European Network and Information Security Agency, *Critical Cloud Computing. A CIIP perspective on cloud computing services*, wersja 1.0 z listopada 2012 r., opublikowana 14 II 2013 r., https://www.enisa.europa.eu/publications/critical-cloud-computing [dostęp: 22 III 2021].

[28] Tamże, s. 6.

obliczeniowej[29]. Propozycje dotyczą jednak głównie powstrzymywania cyberataków. Z zaleceń NSA wynika, że zakłócenia w działalności chmury mogą być wywołane przez wiele rodzajów ataków.

Polskie organy nadzoru również wydają wytyczne w tym zakresie. Na przykład w styczniu 2020 r. Komisja Nadzoru Finansowego (KNF) opublikowała komunikat dotyczący przetwarzania informacji w chmurze obliczeniowej przez nadzorowane przez nią instytucje[30]. Wśród wytycznych związanych z szacowaniem ryzyka wymieniono potrzebę przeprowadzenia oceny, czy stosowane rozwiązania mogą skutkować ryzykiem uzależnienia się od jednego dostawcy. Użytkownik chmury obliczeniowej kontrolowany przez KNF powinien dysponować dokumentacją, która zwiera m.in. scenariusze awaryjne.

Polska planuje wykorzystanie możliwości oferowanych przez rozwiązania chmurowe i stworzenie Rządowej Chmury Obliczeniowej. W związku z tym Rada Ministrów przyjęła we wrześniu 2019 r. uchwałę w sprawie inicjatywy określanej jako „Wspólna Infrastruktura Informatyczna Państwa" (dalej: WIIP). Jednym z pierwszych etapów wprowadzania jej w życie było opublikowanie przez Ministerstwo Cyfryzacji w lutym 2020 r. standardów dotyczących cyberbezpieczeństwa chmur obliczeniowych[31]. Dokument przedstawia wymagania prawne, organizacyjne i techniczne, które muszą zostać spełnione w trakcie projektów wdrażających WIIP. Ze wspomnianej uchwały i standardów wynika, że przynajmniej w sferze deklaratywnej Polska nie tyle chce się uniezależnić od zewnętrznych rozwiązań chmurowych, ile budować je na bazie tych dostarczanych przez dostawców godnych zaufania, pilnować stabilności systemów i na każdym etapie wdrażać zasady cyberbezpieczeństwa.

W sierpniu 2020 r. amerykański think tank Carnegie Endowment for International Peace opublikował materiał na temat bezpieczeństwa chmury, zawierający porady dla polityków[32]. Godny uwagi jest m.in. załącznik, w którym opisano incydenty związane z chmurą i jej awariami[33]. Przedstawiono w nim np. konsekwencje błędu (literówki zrobionej przez programistę Amazona), który w 2017 r. doprowadził do awarii AWS obejmującej całe wschodnie wybrzeże USA. W ostatnich latach do awarii na skalę

---

[29] National Security Agency, *Mitigating Cloud Vulnerabilities*, styczeń 2020 r., https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF [dostęp: 3 III 2021].

[30] *Komunikat Urzędu Komisji Nadzoru Finansowego dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej*, 23 I 2020 r., https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_UKNF_Chmura_Obliczeniowa_68669.pdf [dostęp: 22 III 2021].

[31] *Narodowe Standardy Cyberbezpieczeństwa. Standardy Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO) v. 1.00 – luty 2020*, https://chmura.gov.pl/zuch/static/media/SCCO_v_1.00.pdf [dostęp: 7 VI 2021].

[32] Zob. np. T. Maurer, G. Hinck, *Cloud Security: A Primer for Policymakers*, Carnegie Endowment for International Peace, sierpień 2020, https://carnegieendowment.org/files/Maurer_Hinck_Cloud_Security-V3.pdf [dostęp: 23 III 2021].

[33] Tamże, s. 50–58.

regionalną lub globalną dochodziło także m.in. w wyniku wyładowań atmosferycznych, zmian w konfiguracji serwerów czy nawet zmiany protokołu przesyłania danych przez dostawcę usług internetowych w Nigerii (dane wędrowały okrężną drogą przez Chiny).

Z przedstawionego powyżej przeglądu wynika, że istnieje pewien konsensus na temat tego, że korzystanie z usług chmurowych wiąże się z dwoma poważnymi rodzajami ryzyka. Po pierwsze, usługi chmurowe są narażone na wiele właściwych sobie podatności na błędy i awarie zakłócające ich działanie. Po drugie, dostawca usług chmurowych ma duże możliwości dyskrecjonalnego wpływu na sposób i zakres świadczonych usług. Dlatego tak ważne jest zaufanie do dostawcy, który powinien być partnerem sprawdzonym, rzetelnym i przewidywalnym. Szczególną ostrożność powinno się zachować wobec amerykańskich gigantów technologicznych, o czym przekonują wyniki prac amerykańskiej podkomisji antytrustowej, opisane w dalszej części niniejszego artykułu.

Można zauważyć, że w analizowanej literaturze przedmiotu uwaga została skupiona na bezpośrednich zagrożeniach. Pojawiają się również postulaty akcentujące potrzebę prowadzenia wielopoziomowej analizy problematyki usług chmurowych i zwrócenia uwagi na rosnące znaczenie gospodarcze i polityczne gigantów technologicznych. W przedstawionych poniżej studiach przypadków uwidacznia się problem połączenia czterech filarów zaufania do dostawcy chmury (wskazany przez Schneiera i w pewnym zakresie przez ENISĘ) ze wspomnianym wcześniej trendem dotyczącym konsolidacji zasobów Internetu w rękach wyłaniającego się oligopolu grupy gigantów technologicznych. Wartością dodaną będzie przeanalizowanie, co się dzieje w praktyce, gdy filary zaufania skonceptualizowane przez Schneiera zostają zachwiane przez jedną z najpotężniejszych firm na świecie.

Awaria chmury i efekty kaskadowe jako zakłócenie działania całego Internetu

W dniu 25 listopada 2020 r. w tysiącach gospodarstw domowych na wschodnim wybrzeżu USA przestały działać m.in. inteligentne odkurzacze – roboty sprzątające. Zapewne niewielu ich użytkowników było wtedy świadomych, że przyczyną problemów z domowym AGD jest awaria, która zaistniała u dostawcy usług chmurowych. Skutkiem trwającego kilka godzin uszkodzenia jednej z usług chmurowych Amazona było pojawienie się efektu kaskadowego[34]. Usterka, do której doszło w centrum danych obsługującym wschodnią część USA, zakłóciła działanie aż 27 kolejnych systemów tej firmy związanych z usługami chmurowymi[35]. W konsekwencji ok. 25 firm, także o globalnym zasięgu działania, nie mogło przez co najmniej kilka godzin dostarczać swoim

[34] M. Day, *Amazon Cloud Outage Hits Customers…*

[35] C. Cimpanu, *AWS outage impacts thousands of online services*, Zdnet, 25 XI 2020 r., https://www.zdnet.com/article/aws-outage-impacts-thousands-ofonline-services/ [dostęp: 7 XII 2020].

klientom usług internetowych. Problemy pojawiły się m.in. u dostawców oprogramowania, producenta urządzeń do streamingu telewizji, w urządzeniach Internetu rzeczy (RTV/AGD podłączonych do sieci, w tym we wspomnianych odkurzaczach) oraz u wydawców portali internetowych. Przestały działać również tzw. inteligentne dzwonki do drzwi połączone z kamerami monitoringu, które są produkowane i obsługiwane przez Amazon Ring, spółkę zależną Amazona[36]. Przykład tej awarii pokazuje, że jedna usterka w chmurze obliczeniowej czy też błąd programisty aktualizującego daną usługę może wywołać, niczym poruszenie jednej kostki domina, negatywne skutki w wielu innych elementach struktury.

Podobną reakcję, chociaż na mniejszą skalę, wywołał pożar, który wybuchł w marcu 2021 r. w centrum danych spółki OVH w Strasburgu[37], będącej jednym z mniejszych dostawców usług chmurowych. Wspomniana firma jest jednym z podmiotów zaangażowanych w tworzenie europejskiej chmury w ramach projektu GAIA-X (więcej na temat tego projektu w dalszej części artykułu). Pożar zniszczył jedno centrum danych, a trzy kolejne zostały odcięte od prądu[38]. Z tego powodu wiele portali internetowych doświadczyło przerw w funkcjonowaniu. O nieprzygotowaniu na tego typu awarie wymownie świadczy to, że w jej wyniku administratorzy strony jednej z instytucji publicznych w Polsce – Rzecznika Finansowego – przez kilka dni byli w stanie udostępnić jedynie elementy archiwalnej wersji strony, zachowane dzięki serwisowi Web Archive[39].

Tego rodzaju awarie nie są czymś wyjątkowym. Istotne w powyższych przykładach jest to, że pokazują one rosnącą złożoność usług chmurowych i zależności wynikające z ich wzajemnych połączeń. Im więcej różnych urządzeń jest podłączonych do sieci i im więcej form aktywności człowieka jest realizowanych w sposób zapośredniczony cyfrowo, tym bardziej dalekosiężne i destruktywne mogą być konsekwencje zakłóceń w działaniu chmury.

---

[36] *AWS: Amazon web outage breaks vacuums and doorbells*, BBC, 26 XI 2020 r., https://www.bbc.com/news/technology-55087054 [dostęp: 7 XII 2020].

[37] Zob. np. P. Judge, *Fire destroys OVHCloud's SBG2 data center in Strasbourg*, Data Center Dynamics, 10 III 2021 r., https://www.datacenterdynamics.com/en/news/fire-destroys-ovhclouds-sbg2-data-center-strasbourg/ [dostęp: 24 III 2021].

[38] Jak się później okazało, jeszcze jedno centrum danych nie mogło wznowić działalności. Zob. P. Judge, *OVH fire: OVHcloud abandons efforts to restart SBG1 data center in Strasbourg*, Data Center Dynamics, 21 III 2021 r., https://www.datacenterdynamics.com/en/news/ovh-fire-ovhcloud-abandons-efforts-restart-sbg1-strasbourg/ [dostęp: 24 III 2021].

[39] Zob. https://web.archive.org/web/20210129150346if_/https://rf.gov.pl/ [dostęp: 12 III 2021]. Sprawa została opisana 12 III 2021 r. na blogu „Problemy Polskiej Branży IT", w tekście pt. *Dlaczego admin Rzecznika Finansowego powinien dostać podwyżkę?*, https://ppbit.pl/news/dlaczego-admin-rzecznika-finansowego-powinien-dostac-podwyzke/ [dostęp: 12 III 2021].

Wyłączenie sieci społecznościowej Parler

Na początku stycznia 2021 r., tuż po wtargnięciu tłumu demonstrantów na amerykański Kapitol i zawieszeniu kont Donalda Trumpa w mediach społecznościowych, doszło do zablokowania działania sieci społecznościowej Parler[40]. Skupiała ona m.in. zwolenników kończącego kadencję prezydenta Trumpa, przyciągniętych obietnicą swobodnej wymiany informacji, moderowanej tylko w niewielkim stopniu. Działający od 2018 r. Parler już w listopadzie 2020 r. miał ok. 10 mln użytkowników, z których część została wcześniej usunięta z innych mediów społecznościowych z powodu łamania ich regulaminów[41]. Parler zachęcał do korzystania ze swoich usług, podkreślając, że stosuje liberalne zasady moderacji treści. Miały one bazować głównie na zgłoszeniach od innych użytkowników, którym dane treści wydały się nieodpowiednie. Największy wpływ na zablokowanie Parlera miała decyzja Amazona o zawieszeniu działania infrastruktury tego medium społecznościowego, wykorzystującej chmurę amerykańskiego giganta internetowego. Wspomnianą decyzję ogłoszono bardzo późno – niewiele ponad dobę przed wyłączeniem usług. Amerykańskie media cytowały e-mail wysłany do Parlera przez firmę Amazon[42]. Przedstawicielka tej drugiej spółki wskazywała, że problemem nie było polityczne zaangażowanie użytkowników Parlera, lecz brak odpowiednich mechanizmów blokowania nawoływań do przemocy. W ciągu kilku tygodni poprzedzających zawieszenie Parler miał nie zareagować na 98 zastrzeżeń zgłoszonych przez Amazona do publikowanych na nim treści.

Parler pozwał Amazona i zażądał wstrzymania zawieszenia świadczenia usług chmurowych[43]. Firma argumentowała, że blokada ma podłoże polityczne – jako nowe, konserwatywne medium społecznościowe Parler zaczął się stawać konkurencją dla liberalnego Twittera, który również korzysta z chmury Amazona. Tymczasem, jak można wnioskować z argumentacji Parlera, Twitter także ma problemy z moderacją treści. Decyzja o zawieszeniu Parlera miała wynikać przede wszystkim z chęci uniemożliwienia mu konkurowania z Twitterem. Zgodnie z treścią pozwu zablokowanie korzystania z chmury miało być równoznaczne z (…) *wyciągnięciem wtyczki z maszyny podtrzymującej życie*

[40] B. Fung, *Parler has now been booted by Amazon, Apple and Google*, CNN, 11 I 2021 r., https://edition.cnn.com/2021/01/09/tech/parler-suspended-apple-app-store/index.html [dostęp: 11 I 2021].

[41] J. Schieber, *Parler jumps to No. 1 on App Store after Facebook and Twitter ban Trump*, Tech Crunch, 9 I 2021 r., https://techcrunch.com/2021/01/09/parler-jumps-to-no-1-on-app-store-after-facebook-and-twitter-bans/ [dostęp: 11 I 2021].

[42] Zob. m.in.: J. Paczkowski, R. Mac, *Amazon Is Booting Parler Off Of Its Web Hosting Service*, BuzzFeed, 9 I 2021 r., https://www.buzzfeednews.com/article/johnpaczkowski/amazon-parler-aws [dostęp: 11 I 2021].

[43] Pozew Parlera przeciwko AWS złożony 11 I 2021 r., https://cdn.arstechnica.net/wp-content/uploads/2021/01/gov.uscourts.wawd_.294664.1.0_1.pdf [dostęp: 12 I 2021]. Jedną z analiz pozwu i zawartych w nim argumentów prawnych opracował Mike Masnick. Zob. tenże, *Parler's Laughably Bad Antitrust Lawsuit Against Amazon*, Techdirt, 13 I 2021 r., https://www.techdirt.com/articles/20210113/11333746046/parlers-laughably-bad-antitrust-lawsuit-against-amazon.shtml [dostęp: 14 I 2021].

pacjenta na intensywnej terapii[44]. To porównanie obrazuje niezbędność infrastruktury Amazona dla platformy Parler. Od samego początku jej oprogramowanie i aplikacje na urządzenia mobilne miały być tworzone wyłącznie z myślą o usługach chmurowych Amazona[45]. Nie było więc możliwości ich łatwego przetransferowania na inne platformy, a wybór innego dostawcy wymagał dużych zmian w oprogramowaniu[46]. Parler początkowo twierdził, że jest w stanie bez problemu przejść do innego dostawcy usług chmurowych[47]. Świadczyłoby to o korzystaniu jedynie z infrastruktury AWS. Jednak w pozwach przeciwko Amazonowi firma podkreślała, że jego aplikacja korzystała z rozwiązań typowych dla tego dostawcy usług chmurowych. Oznaczałoby to, że przynajmniej pewne elementy Parlera działały w modelu PaaS.

W odpowiedzi na pozew Parlera Amazon odrzucił wszystkie zarzuty[48]. Dnia 21 stycznia 2021 r. sąd stwierdził, że wniosek o przywrócenie wykonywania usług nie jest zasadny[49]. Do końca stycznia 2021 r. Parlerowi udało się przywrócić działanie portalu tylko w szczątkowej formie[50]. Kolejne amerykańskie firmy dostarczające kompleksowe usługi chmurowe odmówiły z nim współpracy. Konieczne stało się poszukanie mniejszych dostawców poszczególnych usług niezbędnych do reaktywacji portalu. Przykładowo, do zapewnienia ochrony portalu przed atakami typu DDoS (*distributed denial of service*, czyli rozproszona odmowa usługi) Parler wykorzystał rosyjską firmę, która świadczyła usługi m.in. dla Ministerstwa Obrony Federacji Rosyjskiej, spółki zależnej Sbierbanku oraz państwowego dostawcy usług telekomunikacyjnych współpracującego z rosyjskimi służbami specjalnymi[51].

---

[44] Pozew Parlera przeciwko AWS złożony 11 I 2021 r., https://cdn.arstechnica.net/wp-content/uploads/2021/01/gov.uscourts.wawd_.294664.1.0_1.pdf [dostęp: 12 I 2021].

[45] Tamże, s. 5.

[46] Por. D. Cameron, *Every Deleted Parler Post, Many With Users' Location Data, Has Been Archived*, Gizmodo, 11 I 2021 r., https://gizmodo.com/every-deleted-parler-post-many-with-users-location-dat-1846032466 [dostęp: 12 I 2021].

[47] Por. M. Branscombe, *Why Parler Can't Rebuild a Scalable Cloud Service from Scratch*, The New Stack, 19 I 2021 r., https://thenewstack.io/why-parler-cant-rebuild-a-scalable-cloud-service-from-scratch/ [dostęp: 24 III 2021].

[48] Odpowiedź Amazona z 12 I 2021 r. na pozew Parlera, https://beta.documentcloud.org/documents/20449127-amazon_response [dostęp: 13 I 2021]. Por. komentarz do pozwu: T. Sonnemaker, *Amazon hits back at Parler's antitrust lawsuit with extensive examples of its violent content, including death threats against politicians, tech CEOs, and BLM supporters*, Business Inside, 13 I 2021 r., https://www.businessinsider.com/amazon-responds-to-parler-lawsuit-cites-violent-content-section-230-2021-1?IR=T [dostęp: 13 I 2021].

[49] B. Allyn, *Judge Refuses To Reinstate Parler After Amazon Shut It Down*, NPR, 21 I 2021 r., https://www.npr.org/2021/01/21/956486352/judge-refuses-to-reinstate-parler-after-amazon-shut-it-down [dostęp: 23 I 2021].

[50] J. Newman, *Here's why Parler is still struggling to come back online*, Fast Company, 21 I 2021 r., https://www.fastcompany.com/90596427/parler-coming-back-after-aws-ban [dostęp: 23 I 2021].

[51] K. Mehorota, *Parler's New Partner Has Ties to the Russian Government*, Bloomberg, 22 I 2021 r., https://www.bloomberg.com/news/articles/2021-01-22/parler-s-new-partner-has-ties-to-the-russian-government [dostęp: 23 I 2021].

Bezpośrednio przed decyzją Amazona dostęp do aplikacji umożliwiającej korzystanie z Parlera na urządzeniach mobilnych został zawieszony w sklepach z aplikacjami Google Play Store i App Store, z których najłatwiej jest pobrać oprogramowanie na najpopularniejsze urządzenia mobilne (czyli te z systemami operacyjnymi Android oraz iOS). Do zablokowania aplikacji doszło akurat wtedy, gdy w następstwie zawieszenia kont należących do Trumpa Parler stał się najczęściej pobieraną aplikacją w tych dwóch sklepach[52]. O ile usunięcie Parlera ze sklepów z aplikacjami utrudniło dostęp do niego głównie nowym użytkownikom, o tyle zablokowanie możliwości korzystania z chmury Amazona odcięło od tego medium społecznościowego również jego wcześniejszych użytkowników.

Zawieszenie Parlera nie było pierwszą sytuacją, w której doszło do odmowy realizowania usług na rzecz serwisu internetowego przez dostawców infrastruktury sieciowej[53]. Z podobnym problemem nie musiały się jednak mierzyć nigdy dotąd, przynajmniej w USA, największe portale: Facebook, Twitter i YouTube – i to pomimo kłopotów, które te platformy miały w przeszłości i mają obecnie z moderowaniem treści[54]. Przykładowo, w 2018 r. śledczy ONZ zarzucili Facebookowi, że za jego pomocą rozpowszechniano mowę nienawiści, która przyczyniła się do ludobójstwa w Birmie (Mjanma) w 2017 r.[55]

W połowie lutego 2021 r. Parler ponownie uruchomił swoją stronę internetową. Spółka zadeklarowała, że będzie budować infrastrukturę samodzielnie, z pominięciem zasobów Big Tech[56]. Jak się jednak okazało, był to powrót jedynie do nielicznych usług portalu – bez możliwości zapisywania się nowych użytkowników i bez dostępu do archiwalnych dyskusji. To pokazuje, jak trudno jest obecnie samodzielnie zapewnić świadczenie wysokiej jakości usług cyfrowych, bez płacenia za gotową infrastrukturę gigantów cyfrowych. W lutym 2021 r. Apple odmówiło Parlerowi zgody na powrót jego aplikacji do sklepu App Store[57]. Regulamin Parlera w dalszym ciągu miał być w niewystarczającym stopniu zgodny z wymaganiami tego sklepu. W marcu 2021 r. Parler po raz kolejny pozwał Amazona[58]. Zarzucił mu, że wspólnie z innymi (spółki wymienione

---

52 Tamże.

53 G. Edelman, *The Parler Bans Open a New Front in the 'Free Speech' Wars*, Wired, 13 I 2021 r., https://www.wired.com/story/parler-bans-new-chapter-free-speech-wars/ [dostęp: 13 I 2021].

54 Tamże.

55 T. Miles, *U.N. investigators cite Facebook role in Myanmar crisis*, Reuters, 12 III 2018 r., https://www.reuters.com/article/us-myanmar-rohingya-facebook-idUSKCN1GO2PN [dostęp: 14 I 2021].

56 J. Brodkin, *Parler says it's back without 'Big Tech' after being kicked off Amazon*, Ars Technica, 15 II 2021 r., https://arstechnica.com/tech-policy/2021/02/parler-says-its-back-without-big-tech-after-being-kicked-off-amazon/ [dostęp: 3 III 2021].

57 W. Turton, M. Gurman, *Parler Blocked on Apple's App Store After Capitol Riot Review*, Bloomberg, 10 III 2021 r., https://www.bloomberg.com/news/articles/2021-03-10/parler-cuts-ios-team-after-apple-blocks-return-to-app-store [dostęp: 11 III 2021].

58 K. Cox, *Parler sues Amazon (again), claims AWS ban sank a billion-dollar valuation*, Ars Technica, 3 III 2021 r., https://arstechnica.com/tech-policy/2021/03/parler-sues-amazon-again-claims-aws-ban-sank-a-billion-dollar-valuation/ [dostęp: 4 III 2021].

w pozwie to: Twitter, Facebook i Google) postanowił zniszczyć go jako konkurencję[59]. Na skutek zmowy Parler miał stracić szanse na zdobycie inwestorów i to w momencie, gdy był wyceniany na ponad miliard dolarów. Usunięcie go z chmury Amazona sprawiło, że przez ponad miesiąc nie mógł wznowić działalności, stracił klientów i wartość.

Dla niniejszego wywodu nie jest istotne, jak ocenia się działalność Parlera i zagrożenia związane z tą siecią społecznościową. Ważne jest to, że sprawa zablokowania mu możliwości prowadzenia działalności unaoczniła, jak wielką władzę mają dostawcy usług chmurowych. Na przykładzie Parlera widać, że są oni w stanie sparaliżować funkcjonowanie legalnie działającej firmy, która im zaufała. Użyty przez Amazona arbitralny argument o złych mechanizmach moderacji treści, który stał się przesłanką do odcięcia Parlera od usługi chmurowej, może w przyszłości zostać wykorzystany również wobec innych użytkowników chmury Amazona czy innych dostawców. I podobnie jak w wypadku Parlera może się okazać, że oprogramowanie zablokowanego podmiotu było od podstaw zbudowane pod kątem chmury jednego dostawcy. Sama możliwość zaistnienia takiej sytuacji wskazuje na asymetrię relacji pomiędzy dostawcami usług chmurowych a ich klientami.

Funkcjonowanie chmury Amazona w ocenie amerykańskiej podkomisji antytrustowej

W październiku 2020 r. zakończyła swoje postępowanie amerykańska parlamentarna Specjalna Podkomisja ds. Antytrustowych, Konkurencji i Prawa Administracyjnego (Subcommittee on Antitrust, Commercial and Administrative Law), która zbadała działalność Google'a, Apple'a, Facebooka i Amazona pod kątem zagrożeń wolnej konkurencji. W raporcie końcowym stwierdzono, że (…) *firmy te wykorzystują swoją dominację w sposób, który niszczy konkurencyjność, zagraża prywatności Amerykanów w sieci, prowadzi do zaniku wolnych i spluralizowanych mediów. Efektem jest spadek innowacyjności, mniejsza różnorodność oferty rynkowej i osłabienie demokracji* (…). *Potęga tych firm jest zbyt wielka i musi zostać okiełznana poprzez objęcie ich odpowiednim nadzorem i sankcjami*[60].

Przedmiotem badań podkomisji była także działalność chmury Amazona. Jest ona coraz bardziej zyskownym obszarem działalności firmy, gdyż zapewniając 15 proc. przychodów, jednocześnie generuje aż połowę jej dochodu operacyjnego (dane za 2019 r.)[61]. W odniesieniu do AWS we wspomnianym raporcie stwierdza się, że istotnym

[59] Pozew Parlera przeciwko AWS złożony 2 III 2021 r., https://cdn.arstechnica.net/wp-content/uploads/2021/03/parler-llc-v-amazon.pdf [dostęp: 4 III 2021].

[60] Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary, *Investigation of competition in digital markets*, 2020 r., https://int.nyt.com/data/documenttools/house-antitrust-report-on-big-tech/b2ec22cf340e1af1/full.pdf, s. 7 [dostęp: 12 III 2020].

[61] Tamże, s. 316.

problemem jest brak możliwości przenoszenia danych użytkowników między chmurami. Firmy, które próbowały migrować z chmury Amazona do innej, wskazywały, że jest to bardzo trudne i kosztowne[62]. Przyczyną tego zjawiska jest brak interoperacyjności różnych systemów chmurowych. Monopolistyczną pozycję Amazona w tym segmencie rynku utrwala także to, że specjalistów umiejących obsługiwać chmurę tej firmy jest najwięcej, co wynika z jej popularności. Konkurencja wypada pod tym względem znacznie gorzej i jest to kolejna przyczyna, dla której firmom tak trudno jest się przenieść na inne platformy[63]. Dla wielu klientów taka migracja byłaby kosztowna również ze względu na wymuszony przestój w prowadzeniu działalności. W raporcie podkomisja wskazała ponadto, że dzięki wglądowi w szczegóły funkcjonowania infrastruktury chmurowej Amazon ma szeroki dostęp (*near perfect intelligence*) do informacji o całokształcie działalności użytkowników, co zapewnia mu nieuczciwą przewagę nad nimi[64]. Co więcej, firma celowo analizuje działalność swoich kontrahentów, aby tworzyć własną, konkurencyjną ofertę[65]. Klienci usług chmurowych Amazona są często jednocześnie jego konkurentami[66]. Przykładowo, Netflix w 2018 r. zapłacił za korzystanie z chmury AWS pół miliarda dolarów i jednocześnie rywalizował z jego usługą streamingu filmów Amazon Prime Video[67]. Stwierdzono również, że chociaż trudno jest ustalić, jaki dokładnie udział w zapewnianiu usług w chmurze w USA w ramach kontraktów rządowych ma Amazon, to istniejące dane wskazują, że prawdopodobnie jest on największym ich dostawcą. Ponadto jest on (…) *jedynym dostawcą usług w chmurze zapewniającym infrastrukturę niejawną*[68]. Podsumowując wątek Amazona, podkomisja podkreśliła w raporcie: *Ponieważ chmura jest rdzeniem infrastruktury, na której opiera się gospodarka cyfrowa, zapewnienie jej otwartości i konkurencyjności jest najważniejsze*[69]. Tymczasem jak wskazuje przykład Parlera, chmura tej firmy może obecnie nie spełniać tych kryteriów. Można odnieść wrażenie, że przy ustalaniu warunków świadczenia usługi chmurowej Amazon kieruje się dużą uznaniowością w interpretowaniu zapisów umów z klientami.

Kontrakt JEDI na usługi chmurowe dla Departamentu Obrony USA

Ogromnego znaczenia usług w chmurze dla bezpieczeństwa państwa dowodzi kontrakt z 2019 r. dotyczący świadczenia takich usług Departamentowi Obrony USA.

62 Tamże, s. 119.

63 Tamże, s. 319.

64 Tamże, s. 43.

65 Tamże, s. 276.

66 Tamże, s. 318.

67 Tamże, s. 252.

68 Tamże, s. 318.

69 Tamże, s. 325.

Planowanysystem nazwano JEDI (nazwa kojarzy się z filmem *Gwiezdne wojny*). Jest to akronim od *Joint Enterprise Defense Infrastructure*, co można przetłumaczyć jako: infrastruktura dla połączonych przedsięwzięć obronnych. Wartość dziesięcioletniego kontraktu wyceniono na 10 mld dolarów. Zgodnie z oficjalnymi informacjami:

> Chmura JEDI jest inicjatywą, która (…) rozwinie główny system technologii chmurowej dla całego Departamentu [Obrony], ze szczególnym uwzględnieniem dostępności w obszarach, gdzie operują nasze wojska – od działań frontowych do szczebla taktycznego włącznie. Chmura JEDI zapewni (…) usługi dla użytkowników o wszystkich poziomach dostępu do informacji niejawnych. Inicjatywa ta stworzy fundament do skutecznej wymiany informacji poprzez ewolucyjne łączenie różnych domen, zaawansowane zdolności analizy danych i najwyższy poziom cyberbezpieczeństwa[70].

Na zdobywcę tego lukratywnego kontraktu typowano Amazona z uwagi na jego wcześniejsze doświadczenia. W 2013 r. firma podpisała bowiem dziewięcioletni kontrakt na chmurę dla służb specjalnych USA[71]. Wbrew przewidywaniom kontrakt JEDI przypadł Microsoftowi. W marcu 2021 r. nadal trwał spór sądowy pomiędzy tymi firmami dotyczący wspomnianego kontraktu[72], co na pewien czas sparaliżowało postęp prac nad jego wdrożeniem[73].

Atrakcyjność kontraktu JEDI nie wynika wyłącznie z jego wartości finansowej. Wygrywająca go firma stałaby się na dekadę najważniejszym zaufanym partnerem amerykańskiego sektora bezpieczeństwa. W ten sposób zyskałaby szczególną pozycję, nie tylko gospodarczą, lecz także polityczną. Nie bez znaczenia byłaby także możliwość wglądu w kluczowy element infrastruktury krytycznej państwa oraz uzyskanie pewnego zakresu kontroli nad nim.

Wnioski

Jeśli korzystanie z chmury niesie za sobą tyle problemów i zagrożeń, to z czego wynika atrakcyjność rynkowa tego rozwiązania? Światło na to zagadnienie rzuca wywiad

---

[70] *About JEDI Cloud*, https://www.cloud.mil/JEDI-Cloud/ [dostęp: 12 III 2021].

[71] C. Metz, *Amazon's Invasion of the CIA Is a Seismic Shift in Cloud Computing*, Wired, 18 VI 2013 r., https://www.wired.com/2013/06/amazon-cia [dostęp: 6 XI 2020].

[72] Amerykańska armia anulowała zawarty z Microsoftem kontrakt z uwagi na nowe potrzeby armii. Zob. M. Duszczyk, *Pentagon ma problem z Jedi. Amazon bije się z Microsoftem*, cyfrowa.rp.pl, 7 VII 2021 r., https://cyfrowa.rp.pl/globalne-interesy/65535-pentagon-ma-problem-z-jedi-amazon-bije-sie-z-microsoftem [dostęp: 30 VII 2021] – przyp. red.

[73] A. Gregg, *With a $10 billion cloud-computing deal snarled in court, the Pentagon may move forward without it*, „Washington Post", 10 II 2021 r., https://www.washingtonpost.com/business/2021/02/10/jedi-contract-pentagon-biden/ [dostęp: 12 III 2021].

z anonimowym pracownikiem Amazona opublikowany w grudniu 2020 r.[74] Ukazano w nim podejście firmy do jej usług chmurowych. Warto krytycznie odnieść się do tej rozmowy, pamiętając, że strategie tej firmy są zapewne punktem odniesienia dla jej konkurencji.

Do klienta AWS zainteresowanego skorzystaniem z usług chmurowych firmy jest przysyłana (…) *osiemnastokołowa ciężarówka* (…), *modularne centrum danych na kołach, wypełnione dyskami twardymi i przystosowane do podłączenia do centrum danych klienta kablami światłowodowymi. Ta ciężarówka jest strzeżona w czasie transferu i transportu danych przez uzbrojonych strażników*. Jak zauważył pracownik Amazona: (…) *łatwo jest to sprzedać. Jeśli klient przygląda się dostępnym opcjom, to oczywiście, że powie, iż chce wielkiej ciężarówki i uzbrojonych ochroniarzy do transportu danych, a nie jakiś chałowaty system, który opracują na własną rękę*[75]. Ponadto AWS sprzedaje specjalne usługi ułatwiające audyt konfiguracji chmury i rekomendujące możliwości poprawienia ustawień. W ten sposób sprawia, że jego klienci nie muszą dbać o zatrudnianie fachowców, którzy byliby w stanie sami przeprowadzić taką analizę i następnie wdrożyć odpowiednie rozwiązania. Ponadto chmura Amazona pozwala klientom na *outsourcing* przestrzegania regulacji związanych z prywatnością danych. Chodzi tu także o europejskie przepisy, takie jak RODO czy prawo do bycia zapomnianym, rozumiane jako prawo do usunięcia linków do określonych stron z wyników wyszukiwania w danej wyszukiwarce.

Podmiot chcący konkurować w ramach współczesnej gospodarki cyfrowej stoi przed dylematem. Jeśli chce zapewnić jakość usług, do której coraz więcej klientów jest przyzwyczajonych, to przede wszystkim musi zadbać o szybkość i płynność działania interfejsu, jego dostępność z poziomu różnych typów urządzeń, stabilność, niezawodność i bezpieczeństwo danych oraz dokonywanych transakcji. Samodzielne rozwijanie takiego systemu przekracza możliwości wielu nawet dużych podmiotów, a ponadto tego typu próby są obarczone dużym ryzykiem porażki. Alternatywą jest zdanie się na gotowy system, sprawdzony i gwarantowany przez renomowanych dostawców usług chmurowych.

Przed podobnymi dylematami jak firmy stoją państwa i organizacje międzynarodowe. Polski projekt Chmury Krajowej i europejska inicjatywa chmury obliczeniowej znana pod nazwą GAIA-X (wspierana przez Komisję Europejską) to przykłady poważnych trudności z uniezależnieniem się od usług chmurowych oferowanych przez Big Tech. Przedstawiciele rządów oraz firm sektora IT z Niemiec i Francji opublikowali w lutym 2020 r. standardy, według których mógłby funkcjonować projekt GAIA-X[76]. Obejmują one m.in. możliwość zmiany operatora usług chmurowych, europejski system certyfikacji dostawców oraz ochronę przed dostępem do danych przechowywanych

[74] *Inside the Whale: An Interview with an Anonymous Amazonian*, „Logic" 2020, nr 12, 20 XII 2020 r., https://logicmag.io/commons/inside-the-whale-an-interview-with-an-anonymous-amazonian/ [dostęp: 20 III 2021].

[75] Tamże.

[76] *Franco-German Position on GAIA-X*, 19 II 2020 r., https://www.bmwi.de/Redaktion/DE/Downloads/F/franco-german-position-on-gaia-x.pdf?__blob=publicationFile&v=10 [dostęp: 9 III 2020].

w europejskiej chmurze państw spoza Unii. GAIA-X od początku jej tworzenia ma zakładać suwerenność danych (*data sovereignty by design*). W lutym 2020 r. Microsoft ujawnił, że prowadzi negocjacje z niemieckim ministerstwem gospodarki w sprawie możliwego udziału w GAIA-X[77]. Europejski projekt miał być próbą stworzenia konkurencji dla amerykańskich dostawców, dla których jedyną realną alternatywą jest obecnie chiński Alibaba. Udział Microsoftu w projekcie budzi jednak wątpliwości co do prawdziwości deklaracji o dążeniu do zapewnienia autonomii strategicznym usługom chmurowym. Podobnie jest w przypadku projektu polskiej Chmury Krajowej, w którym partnerami strategicznymi są Microsoft i Google Cloud[78].

Na przykładzie przedsięwzięć GAIA-X oraz Chmura Krajowa widać, że dążenia do suwerenności cyfrowej polegające na opracowywaniu własnych rozwiązań chmurowych napotykają duże trudności w postaci braku samowystarczalności w tym zakresie. W praktyce oznacza to skazanie na korzystanie z oferty amerykańskich, chińskich czy rosyjskich gigantów technologicznych. Fakt, że globalny rynek usług chmurowych jest w rzeczywistości oligopolem zdominowanym przez kilka podmiotów, każe zastanowić się nad kierunkiem, w którym podążają zmiany w strukturze współczesnej sieci. Internet powstał jako sieć zdecentralizowana i rozproszona, a więc taka, w której awaria czy zniszczenie poszczególnych węzłów nie powinny mieć istotnego znaczenia dla funkcjonowania całości. Opisane w niniejszym artykule awarie usług chmurowych Amazona oraz konsekwencje jego arbitralnej decyzji o zakończeniu realizowania usługi dla klienta mogą być uznane za symptomy niebezpiecznej ewolucji Internetu w stronę struktury bardziej scentralizowanej, a zatem w większym stopniu podatnej na awarie najważniejszych węzłów, sabotaż czy cyberataki. Obecnie nie można określić, jak poważne konsekwencje mogłaby mieć awaria chmury Amazona lub jego – niekoniecznie największych – konkurentów.

Trend nieoczekiwanej recentralizacji struktury sieci jest szerszy i nie dotyczy tylko usług chmurowych. Eksperci wskazują na pojawienie się zjawiska określanego jako Splinternet[79], bałkanizacja sieci[80] lub nacjonalizacja – czyli wydzielenie się Internetu chińskiego, rosyjskiego czy też ostatnio indyjskiego. Im więcej sfer życia współczesnego człowieka jest zapośredniczanych cyfrowo przez korzystanie z urządzeń podłączonych do sieci, tym większe znaczenie dla globalnego środowiska bezpieczeństwa

---

[77] S. Stolton, *Microsoft 'in discussions' with Germans on Gaia-X participation*, 25 II 2020 r., https://www.euractiv.com/section/digital/news/microsoft-in-discussions-with-germans-on-gaia-x-participation/ [dostęp: 9 III 2020].

[78] A. Marczyński, *Na Podsłuchu, odcinek 33 – ten o Chmurze Krajowej i jej bezpieczeństwie*, rozmawiał Piotr Konieczny, Niebezpiecznik, 24 III 2021 r., https://niebezpiecznik.pl/post/na-podsluchu-odcinek-33-ten-o-chmurze-krajowej-i-jej-bezpieczenstwie/ [dostęp: 29 III 2021]; por. https://chmura-krajowa.pl/dlaczego-chmura-krajowa/ [dostęp: 29 III 2021].

[79] L.S., *What is the 'splinternet'?*, „The Economist", 22 XI 2016 r., https://www.economist.com/the-economist-explains/2016/11/22/what-is-the-splinternet [dostęp: 29 III 2021].

[80] B. Sajduk, *Chiński krok w stronę bałkanizacji Internetu*, Nowa Konfederacja, 14 IX 2020 r., https://nowakonfederacja.pl/chinski-krok-w-strone-balkanizacji-internetu/ [dostęp: 29 III 2021].

ma niezakłócone funkcjonowanie Internetu. Trend polegający na jego strukturalnej recentralizacji w postaci umacniania się oligopolu dostawców usług chmurowych zwiększa podatność na destabilizację. Jeżeli do wywołania efektu kaskadowego paraliżującego działania dużych obszarów sieci może przyczynić się prosty błąd programisty, to należy się spodziewać, że podobny efekt może być wywołany intencjonalnie – przez cyberatak. W tym sensie zjawisko polegające na tym, że usługi w chmurze stają się w coraz większym stopniu niewidzialną infrastrukturą Internetu, prowadzi do powstania nowych podatności na destabilizację globalnego środowiska bezpieczeństwa.

Bibliografia

Almorsy M., Grundy J., Müller I., *An analysis of the cloud computing security problem*, w: *Proceedings of the APSEC 2010 Cloud Workshop*, Sydney 2010.

Delamore B., Ko Ryan K.L., *Security as a service (SECaaS) – An overview*, w: *The Cloud Security Ecosystem. Technical, Legal, Business and Management Issues*, Ryan Ko, Kim-Kwang Raymond Choo (red.), Waltham 2015, Syngress, s. 187–202.

Gunawi H.S. i in., *Why Does the Cloud Stop Computing? Lessons from Hundreds of Service Outages*, w: *Proceedings of the Seventh ACM Symposium on Cloud Computing (SoCC '16)*, New York 2016, Association for Computing Machinery, s. 1–16.

Gurtowski M., Waszewski J., *Wpływ działalności gigantów technologicznych na globalne środowisko bezpieczeństwa. Studium przypadku spółki Amazon*, „Kwartalnik Bellona" 2020, nr 3, s. 37–56.

Kandukuri B.R., Paturi R.V., Rakshit A., *Cloud Security Issues*, w: *Procedings of the 2009 IEEE International Conference on Services Computing*, Washington 2009, IEEE Computer Society, s. 517–520, https://ieeexplore.ieee.org/document/5283911 [dostęp: 23 VII 2021].

Kemmericha T., Agrawala V., Momsen C., *Secure migration to the cloud – In and out*, w: *The Cloud Security Ecosystem. Technical, Legal, Business and Management Issues*, Ryan Ko, Kim-Kwang Raymond Choo (red.), Waltham 2015, Syngress, s. 205–230.

Ko Ryan, Choo Kim-Kwang Raymond, *Cloud Security Ecosystem*, w: *The Cloud Security Ecosystem. Technical, Legal, Business and Management Issues*, Ryan Ko, Kim-Kwang Raymond Choo (red.), Waltham 2015, Syngress, s. 1–14.

Ramgovind S., Eloff M.M., Smith E., *The Management of Security in Cloud Computing*, w: *2010 Information Security for South Africa (ISSA 2010)*, 2010 r., Institute of Electrical and Electronics Engineers.

Stake R.E., *Jakościowe studium przypadku*, w: *Metody badań jakościowych*, N.K. Denzim, Y.S. Lincoln (red.), Warszawa 2009, t. 1, s. 623–654.

Tang S., *A systemic theory of the security environment*, „Journal of Strategic Studies" 2004, nr 1, s. 1–34.

The Cloud Security Ecosystem. Technical, Legal, Business and Management Issues, Ryan Ko, Kim-Kwang Raymond Choo (red.), Waltham 2015, Syngress.

Turbiville G.H., Mendel W.W., Kipp J.W., *The Changing security environment*, „Military Review" 1997, nr 77, s. 5–10.

Źródła internetowe

About JEDI Cloud, https://www.cloud.mil/JEDI-Cloud/ [dostęp: 12 III 2021].

Allyn B., *Judge Refuses To Reinstate Parler After Amazon Shut It Down*, NPR, 21 I 2021 r., https://www.npr.org/2021/01/21/956486352/judge-refuses-to-reinstate-parler-after-amazon-shut-it-down [dostęp: 23 I 2021].

AWS: Amazon web outage breaks vacuums and doorbells, BBC, 26 XI 2020 r., https://www.bbc.com/news/technology-55087054 [dostęp: 7 XII 2020].

Branscombe M., *Why Parler Can't Rebuild a Scalable Cloud Service from Scratch*, The New Stack, 19 I 2021 r., https://thenewstack.io/why-parler-cant-rebuild-a-scalable-cloud-service-from-scratch/ [dostęp: 24 III 2021].

Brodkin J., *Parler says it's back without 'Big Tech' after being kicked off Amazon*, Ars Technica, 15 II 2021 r., https://arstechnica.com/tech-policy/2021/02/parler-says-its-back-without-big-tech-after-being-kicked-off-amazon/ [dostęp: 3 III 2021].

Cameron D., *Every Deleted Parler Post, Many With Users' Location Data, Has Been Archived*, Gizmodo, 11 I 2021 r., https://gizmodo.com/every-deleted-parler-post-many-with-users-location-dat-1846032466 [dostęp: 12 I 2021].

Centrum Doktryn i Szkolenia Sił Zbrojnych, *Analiza środowiska bezpieczeństwa w perspektywie 2035 r.*, Bydgoszcz 2020, https://cdissz.wp.mil.pl/pl/articlespublikacje_cdissz/analiza-srodowiska-bezpieczenstwa-w-perspektywie-2035-roku-pl/ [dostęp: 24 III 2021].

Cimpanu C., *AWS outage impacts thousands of online services*, Zdnet, 25 XI 2020 r., https://www.zdnet.com/article/aws-outage-impacts-thousands-ofonline-services/ [dostęp: 7 XII 2020].

Co to jest kontener?, https://azure.microsoft.com/pl-pl/overview/what-is-a-container/ [dostęp: 24 III 2021].

Cox K., *Parler sues Amazon (again), claims AWS ban sank a billion-dollar valuation*, Ars Technica, 3 III 2021 r., https://arstechnica.com/tech-policy/2021/03/parler-sues-amazon-again-claims-aws-ban-sank-a-billion-dollar-valuation/ [dostęp: 4 III 2021].

Day M., *Amazon Cloud Outage Hits Customers Including Roku, Adobe*, Bloomberg, 25 XI 2020 r., https://www.bloomberg.com/news/articles/2020-11-25/amazon-web-services-outage-hits-cloud-customers [dostęp: 7 XII 2020].

Del Rey J., *Amazon's massive AWS outage was caused by human error*, Recode, 2 III 2017 r., https://www.vox.com/2017/3/2/14792636/amazon-aws-internetoutage-cause-human-error-incorrect-command [dostęp: 11 XII 2020].

Duszczyk M., *Pentagon ma problem z Jedi. Amazon bije się z Microsoftem*, cyfrowa.rp.pl, 7 VII 2021 r., https://cyfrowa.rp.pl/globalne-interesy/65535-pentagon-ma-problem-z-jedi-amazon-bije-sie-z-microsoftem [dostęp: 30 VII 2021].

Dlaczego admin Rzecznika Finansowego powinien dostać podwyżkę?, Problemy Polskiej Branży IT, 12 III 2021 r., https://ppbit.pl/news/dlaczego-admin-rzecznika-finansowego-powinien-dostac-podwyzke/ [dostęp: 12 III 2021].

Edelman G., *The Parler Bans Open a New Front in the 'Free Speech' Wars*, Wired, 13 I 2021 r., https://www.wired.com/story/parler-bans-new-chapter-free-speech-wars/ [dostęp: 13 I 2021].

European Network and Information Security Agency, *Cloud Computing. Benefits, risks and recommendations for information security*, rev. B z grudnia 2012 r., https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks--and-recommendations-for-information-security/at_download/file [dostęp: 22 III 2021].

European Network and Information Security Agency, *Critical Cloud Computing. A CIIP perspective on cloud computing services*, wersja 1.0 z listopada 2012 r., opublikowana 14 II 2013 r., https://www.enisa.europa.eu/publications/critical-cloud-computing/at_download/fullReport [dostęp: 22 III 2021].

Franco-German Position on GAIA-X, 19 II 2020 r., https://www.bmwi.de/Redaktion/DE/Downloads/F/franco-german-position-on-gaia-x.pdf?__blob=publicationFile&v=10 [dostęp: 9 III 2020].

Fung B., *Parler has now been booted by Amazon, Apple and Google*, CNN, 11 I 2021 r., https://edition.cnn.com/2021/01/09/tech/parler-suspended-apple-app-store/index.html [dostęp: 11 I 2021].

Global cloud services market Q4 2020, Canalys, 2 II 2021 r., https://www.canalys.com/newsroom/global-cloud-market-q4-2020 [dostęp: 5 III 2021].

Gregg A., *With a $10 billion cloud-computing deal snarled in court, the Pentagon may move forward without it*, „Washington Post", 10 II 2021 r., https://www.washingtonpost.com/business/2021/02/10/jedi-contract-pentagon-biden/ [dostęp: 12 III 2021].

Gürses S., Van Hoboken J., *Privacy After the Agile Turn*, w: *Cambridge Handbook of Consumer Privacy*, J. Polonetsky, O. Tene, E. Selinger (red.), Cambridge 2017, Cambridge University Press, https://osf.io/preprints/socarxiv/9gy73/ lub https://osf.io/ufdvb/ [dostęp: 22 III 2021].

Hill K., *Goodbye Big Five*, Gizmodo, 7 II 2019 r., https://gizmodo.com/c/goodbye-big-five [dostęp: 4 III 2021].

Hill K., *I Tried to Block Amazon From My Life. It Was Impossible*, Gizmodo, 22 I 2019 r., https://gizmodo.com/i-tried-to-block-amazon-from-my-life-it-was-impossible-1830565336 [dostęp: 24 III 2021].

Inside the Whale: An Interview with an Anonymous Amazonian, „Logic" 2020, nr 12, https://logicmag.io/commons/inside-the-whale-an-interview-with-an-anonymous-amazonian/ [dostęp: 20 III 2021].

Judge P., *Fire destroys OVHCloud's SBG2 data center in Strasbourg*, Data Center Dynamics, 10 III 2021 r., https://www.datacenterdynamics.com/en/news/fire-destroys-ovhclouds-sbg2-data-center-strasbourg/ [dostęp: 24 III 2021].

Judge P., *OVH fire: OVHcloud abandons efforts to restart SBG1 data center in Strasbourg*, Data Center Dynamics, 21 III 2021 r., https://www.datacenterdynamics.com/en/news/ovh-fire-ovhcloud-abandons-efforts-restart-sbg1-strasbourg/ [dostęp: 24 III 2021].

Komunikat Urzędu Komisji Nadzoru Finansowego dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej, 23 I 2020 r., https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_UKNF_Chmura_Obliczeniowa_68669.pdf [dostęp: 22 III 2021].

L.S., *What is the "splinternet"?*, „The Economist", 22 XI 2016 r., https://www.economist.com/the-economist-explains/2016/11/22/what-is-the-splinternet [dostęp: 29 III 2021].

Marczyński A., *Na Podsłuchu, odcinek 33 – ten o Chmurze Krajowej i jej bezpieczeństwie*, Niebezpiecznik, 24 III 2021 r., https://niebezpiecznik.pl/post/na-podsluchu-odcinek-33-ten-o-chmurze-krajowej-i-jej-bezpieczenstwie/ [dostęp: 29 III 2021].

Masnick M., *Parler's Laughably Bad Antitrust Lawsuit Against Amazon*, Techdirt, 13 I 2021 r., https://www.techdirt.com/articles/20210113/11333746046/parlers-laughably-bad-antitrust-lawsuit-against-amazon.shtml [dostęp: 14 I 2021].

Maurer T., Hinck G., *Cloud Security: A Primer for Policymakers*, Carnegie Endowment for International Peace, sierpień 2020 r., https://carnegieendowment.org/files/Maurer_Hinck_Cloud_Security-V3.pdf [dostęp: 23 III 2021].

Mehorota K., *Parler's New Partner Has Ties to the Russian Government*, Bloomberg, 22 I 2021 r., https://www.bloomberg.com/news/articles/2021-01-22/parler-s-new-partner-has-ties-to-the-russian-government [dostęp: 23 I 2021].

Mell P., Grance T., *The NIST Definition of Cloud Computing*, wrzesień 2011 r., https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf [dostęp: 4 III 2021].

Metz C., *Amazon's Invasion of the CIA Is a Seismic Shift in Cloud Computing*, Wired, 18 VI 2013 r., https://www.wired.com/2013/06/amazon-cia [dostęp: 6 XI 2020].

Miles T., *U.N. investigators cite Facebook role in Myanmar crisis*, Reuters, 12 III 2018 r., https://www.reuters.com/article/us-myanmar-rohingya-facebook-idUSKCN1GO2PN [dostęp: 14 I 2021].

Mitigating Cloud Vulnerabilities, National Security Agency, styczeń 2020 r., https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF [dostęp: 3 III 2021].

Narodowe Standardy Cyberbezpieczeństwa. Standardy Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO) v. 1.00 – luty 2020, https://chmura.gov.pl/zuch/static/media/SCCO_v_1.00.pdf [dostęp: 7 VI 2021].

Newman J., *Here's why Parler is still struggling to come back online*, Fast Company, 21 I 2021 r., https://www.fastcompany.com/90596427/parler-coming-back-after-aws-ban [dostęp: 23 I 2021].

Odpowiedź Amazona z 12 I 2021 r. na pozew Parlera, https://beta.documentcloud.org/documents/20449127-amazon_response [dostęp: 13 I 2021].

Paczkowski J., Mac R., *Amazon Is Booting Parler Off Of Its Web Hosting Service*, BuzzFeed, 9 I 2021 r., https://www.buzzfeednews.com/article/johnpaczkowski/amazon-parler-aws [dostęp: 11 I 2021].

Pozew Parlera przeciwko AWS złożony 11 I 2021 r., https://cdn.arstechnica.net/wp-content/uploads/2021/01/gov.uscourts.wawd_.294664.1.0_1.pdf [dostęp: 12 I 2021].

Pozew Parlera przeciwko AWS złożony 2 III 2021 r., https://cdn.arstechnica.net/wp-content/uploads/2021/03/parler-llc-v-amazon.pdf [dostęp: 4 III 2021].

Sajduk B., *Chiński krok w stronę bałkanizacji Internetu*, Nowa Konfederacja, 14 IX 2020 r., https://nowakonfederacja.pl/chinski-krok-w-strone-balkanizacji-internetu/ [dostęp: 29 III 2021].

Schieber J., *Parler jumps to No. 1 on App Store after Facebook and Twitter ban Trump*, Tech Crunch, 9 I 2021 r., https://techcrunch.com/2021/01/09/parler-jumps-to-no-1-on-app-store-after-facebook-and-twitter-bans/ [dostęp: 11 I 2021].

Schneier B., *Cloud Computing*, Schneier on Security, 4 VI 2009 r., https://www.schneier.com/blog/archives/2009/06/cloud_computing.html [dostęp: 17 III 2021].

Sonnemaker T., *Amazon hits back at Parler's antitrust lawsuit with extensive examples of its violent content, including death threats against politicians, tech CEOs, and BLM supporters*, Business Insider, 13 I 2021 r., https://www.businessinsider.com/amazon-responds-to-parler-lawsuit-cites-violent-content-section-230-2021-1?IR=T [dostęp: 13 I 2021].

Stolton S., *Microsoft 'in discussions' with Germans on Gaia-X participation*, 25 II 2020 r., https://www.euractiv.com/section/digital/news/microsoft-in-discussions-with-germans-on-gaia-x-participation/ [dostęp: 9 III 2020].

Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary, *Investigation of competition in digital markets*, 2020 r., https://int.nyt.com/data/documenttools/house-antitrust-report-on-big-tech/b2ec22cf340e1af1/full.pdf [dostęp: 12 III 2020].

Taylor L., *Public Actors Without Public Values: Legitimacy, Domination and the Regulation of the Technology Sector*, „Philosophy & Technology", 20 I 2021 r., https://link.springer.com/article/10.1007/s13347-020-00441-4 [dostęp: 22 III 2021].

Turton W., Gurman M., *Parler Blocked on Apple's App Store After Capitol Riot Review*, Bloomberg, 10 III 2021 r., https://www.bloomberg.com/news/articles/2021-03-10/parler-cuts-ios-team-after-apple-blocks-return-to-app-store [dostęp: 11 III 2021].

Abstrakt

Zakłócenia w działaniu chmury obliczeniowej są bardzo ważnym zjawiskiem z perspektywy globalnego środowiska bezpieczeństwa. W artykule przedstawiono analizę tego problemu, wykorzystując w tym celu metodę studium przypadków. Opisano dwa incydenty o daleko idących konsekwencjach, które jednocześnie są dość typowe dla prezentowanych w literaturze przedmiotu. Po pierwsze, na przykładzie jednej z awarii globalnego dostawcy usług chmurowych omówiono problem rosnącej złożoności usług tego typu. Sprawia ona, że nawet drobna awaria jednego z elementów chmury może wywołać efekty kaskadowe i zakłócenia pracy wielu podmiotów. Po drugie, na przykładzie zablokowania działania sieci społecznościowej Parler przeanalizowano problem uzależnienia się klientów od usług danego dostawcy chmury. To powiązanie powoduje, że niezakłócona migracja do innego dostawcy jest utrudniona, jeśli w ogóle możliwa. Oba wskazane problemy były dotychczas analizowane głównie z perspektywy zagrożeń przedsiębiorstw, np. pod kątem kontynuacji działalności, cyberbezpieczeństwa lub naruszeń prywatności. Pomijany był natomiast fakt, że usługi chmurowe stają się stopniowo niewidzialną infrastrukturą Internetu, co ma niebagatelne znaczenie dla środowiska bezpieczeństwa.

Słowa kluczowe: chmura obliczeniowa, infrastruktura krytyczna, cyberbezpieczeństwo.

The invisible Internet infrastructure – cloud services as a critical element of the security environment. The Amazon case

Abstract

The disruptions in cloud computing are an important aspect in the global security environment. An instrumental case study method has been used to analyse this problem. Two relevant examples are discussed which are typical of literature in the field. Firstly, the problem of the growing complexity of the cloud is described. One of the service outages of a global cloud provider is used as an example. It indicates that even relatively small failures might trigger a cascade effect and far-reaching breakdowns. Secondly, the suspension and – as the result of this suspension – the standstill of the social media company Parler is analysed. It is used as the example of the so-called vendor lock-in problem in cloud computing, which renders undisrupted migration to other vendors particularly hard – and at times even impossible. Aforementioned issues have been so far studied mostly from the perspective of the continuity of enterprises, cybersecurity, or privacy. The key phenomenon crucial for the global security environment is usually omitted, namely that the cloud computing has become "the Internet's invisible infrastructure".

Keywords: cloud computing, critical infrastructure, cybersecurity.