



INSTYTUT JAGIELLOŃSKI

CHMURA OBLICZENIOWA W ENERGETYCE

EMANUEL WANAT
PATRYCJA IGNASZAK
BARTŁOMIEJ BARTNICKI

2021

CHMURA OBLICZENIOWA W ENERGETYCE

EMANUEL WANAT
PATRYCJA IGNASZAK
BARTŁOMIEJ BARTNICKI

©Copyright by Instytut Jagielloński
Warszawa, marzec 2021



Instytut Jagielloński
ul. Marszałkowska 84/92 lok. 115
00-514 Warszawa

jagiellonski.pl
instytut@jagiellonski.pl

PROJEKT I PRODUKCJA:
PIOTR PERZYNA

 **NOWEMEDIA24.PL**

PARTNER RAPORTU:



CHMURA OBLICZENIOWA W ENERGETYCE

EMANUEL WANAT
PATRYCJA IGNASZAK
BARTŁOMIEJ BARTNICKI

SPIS TREŚCI

| | |
|---|-----------|
| 1. Wstęp | 6 |
| 2. Executive Summary | 8 |
| Wnioski raportu | 9 |
| 3. Czym jest chmura obliczeniowa? | 10 |
| 3.1. Definicja; cechy | 12 |
| 3.2. Przykładowe elementy systemów IT podlegające migracji | 15 |
| 4. Światowe trendy | 17 |
| 4.1. Wykorzystanie chmury w sektorze prywatnym | 18 |
| 4.2. Chmura a państwowe strategie cyfryzacji i cyberbezpieczeństwa | 20 |
| 4.2.1. Działania na poziomie europejskim | 20 |
| 4.2.2. Działania władz polskich | 23 |
| 4.3. Wdrożenie chmury obliczeniowej w wybranych organizacjach (<i>case studies</i>) | 24 |

| | |
|--|-----------|
| 5. Polska energetyka w chmurze | 31 |
| 5.1. Wstęp; specyfika sektora energetyki | 32 |
| 5.2. Ocena przydatności chmury obliczeniowej | 32 |
| 5.2.1. Czy korzystanie z chmury obliczeniowej w energetyce jest zgodne z prawem? | 36 |
| 5.2.2. Czy korzystanie z chmury obliczeniowej nie zagraża bezpieczeństwu danych? | 41 |
| 5.2.3. Czy korzystanie z chmury obliczeniowej „się opłaca”? | 44 |
| 5.2.4. Czy moja organizacja niesłusznie obawia się wdrożenia chmury? | 48 |
| 6. Podsumowanie i rekomendacje | 55 |



1. WSTĘP

Rynek rozwiązań chmurowych jest jednym z najszybciej rozwijających się na świecie. Prognozuje się, że z uwagi na pandemię do 2022 r. ponad 90% światowych przedsiębiorstw będzie korzystać z różnego rodzaju usług chmury. W latach 2020-2027 światowy rynek chmury¹ wzrośnie z poziomu 313,1 miliardów USD w 2020 r. do 937,5 miliardów USD w 2027 r., osiągając CAGR na poziomie 17%².

Pomimo tego, chmura nie doczekała się powszechnej adopcji w energetyce, a według dostępnych danych jedynie co trzeci przedsiębiorca z sektora *utilities* w Polsce korzysta z tego typu rozwiązań. Wskazywane obawy hamujące szerszą implementację chmury obejmują m.in. niepewność stanu prawnego, obawę o wysokie koszty inwestycji czy bezpieczeństwo danych.

Polska energetyka stoi jednak przed wyzwaniami, które wymuszają elastyczne podejście do nowych technologii. Pandemia koronawirusa wymusiła na organizacjach pracę zdalną, a zmiany w tym zakresie mogą mieć charakter długoterminowy. Konsumenci stają się coraz bardziej świadomi i aktywni, poszukując informacji o tym skąd pochodzi dostarczana im energia, jak została wytworzona i jak wpływa na ich zdrowie³. Energetyka jako sektor fundamentalny dla bezpieczeństwa państwa i gospodarki, staje się coraz częściej celem ataków hakerskich. Stoi więc przed wyzwaniem poszukiwania innowacji, bez jednoczesnego osłabienia bezpieczeństwa systemu. Dalszy rozwój nieuchronnie związany będzie z uzyskaniem zdolności analizy coraz większych ilości danych, prowadzenia procesów badawczych R&D w zakresie uczenia maszynowego i big data.

W tych okolicznościach, chmura może odgrywać kluczową rolę w rozwoju spółek energetycznych. Z rozwiązań chmurowych korzystają dziś zarówno światowi giganci energetyki, jak i niektóre polskie spółki. Chmura wpisuje się w europejskie strategie rozwoju i cyfryzacji, a związane z nią korzyści obejmują m.in. elastyczne zarządzanie zasobami, potencjalne ograniczenie nakładów inwestycyjnych i dostęp do praktycznie nieograniczonych mocy obliczeniowych. Raport ma na celu przybliżenie zagadnienia chmury obliczeniowej, zobrazowanie miejsca polskiego sektora energetycznego w świecie cyfrowej rewolucji i dokonanie bilansu korzyści oraz wad tej technologii.

1 Zob. International Data Corporation, <https://www.idc.com/getdoc.jsp?containerId=prMETA46165020>.

2 Zob. https://www.reportlinker.com/p0197184/Global-Cloud-Computing-Services-industry.html?utm_source=GNW; według innych źródeł światowy rynek usług chmury do 2023 r. osiągnie wartość 266 miliardów dolarów: <https://hostingtribunal.com/blog/cloud-adoption-statistics/>.

3 Wyzwania branży energetycznej w ramach zrównoważonego rozwoju, Analiza tematyczna nr 2/2016, Forum Odpowiedzialnego Biznesu.



2.

EXECUTIVE SUMMARY

Wnioski raportu:

1. *Cloud computing* to w uproszczeniu technologia określająca nowoczesny model przetwarzania danych. Jego głównym założeniem jest udostępnianie zasobów obliczeniowych (infrastruktury, oprogramowania, sprzętu) „na żądanie”. Usługi są dostarczane przy wykorzystaniu serwerów dostawcy za pomocą Internetu. Zasoby mogą być dynamicznie dostosowywane do potrzeb użytkownika (np. pod względem liczby licencji, mocy obliczeniowej) bez ingerencji usługodawcy. Usługi są zwykle rozliczane w formie regularnych opłat (abonamentu).
2. Wykorzystanie chmury pozwala na uzyskanie dostępu do oprogramowania zewnętrznego dostawcy, m.in. na potrzeby: (I) przechowywania plików, (II) korzystania z aplikacji biurowych i skrzynki email, (III) korzystania z dedykowanych aplikacji typu ERP, SAP, CRM, (IV) uruchamiania rozmaitych procesów i wykonywania obliczeń w infrastrukturze dostawcy. Korzyści obejmują m.in.: zapewnienie dostępu do elastycznych, multiplatformowych usług ułatwiających pracę zdalną i kolaborację organizacji (modern *workplace*); potencjalne zmniejszenie kosztów systemów IT; dostęp do narzędzi pozwalających na analizę dużej ilości danych w czasie rzeczywistym; potencjalne zwiększenie bezpieczeństwa danych.
3. Kluczową zaletą chmury jest jej skalowalność i dynamiczna alokacja zasobów. Tradycyjnie, przedsiębiorstwa sektora energetyki muszą być przygotowane na scenariusze krytyczne. Przykładowo, silne wiatry mogą doprowadzić do zerwania lokalnej sieci elektroenergetycznej; w takim przypadku dystrybutor energii otrzyma w krótkim czasie kilkanaście tysięcy zgłoszeń awarii z jednego regionu. Obsłużenie tego typu zdarzenia (analiza, przyjęcie zgłoszenia, organizacja usuwania awarii, odpowiedzi na zgłoszenia) wymaga dużej mocy obliczeniowych, wielokrotnie wyższych niż w codziennej pracy organizacji. Dlatego też, wielu przedsiębiorców nabywa infrastrukturę znacznie przewyższającą ich regularne potrzeby, tylko po to, żeby być przygotowanym na zdarzenia kryzysowe. W efekcie, ponoszą wysokie nakłady inwestycyjne na infrastrukturę, która regularnie wykorzystywana jest jedynie w 30-40%. Chmura pozwala na odwrócenie tego mechanizmu. Usługi dostarczane są w modelu „na żądanie” i dostosowane do potrzeb użytkownika, który uzyskuje możliwość dynamicznej zmiany wykorzystywanych zasobów w zależności od okoliczności i potrzeb, bez konieczności angażowania dostawcy.
4. Korzystanie z chmury w Polsce pozostaje na stosunkowo niskim poziomie. W sektorze *utilities* co trzeci przedsiębiorca korzysta z tej technologii. Analiza *case studies* wdrożenia chmury przez wybrane przedsiębiorstwa energetyczne (krajowe i zagraniczne) dowodzi jednak, że **technologia ta może być atrakcyjnym rozwiązaniem dla sektora, pozwalającym na poprawę innowacyjności i zwiększenie odporności na sytuacje kryzysowe**. Implementacja chmury wpisuje się w światowe i europejskie trendy.
5. Pandemia koronawirusa niewątpliwie pokazała, jak ważne usługi chmury mogą okazać się w najbliższej przyszłości. Przedsiębiorstwa korzystające z chmury bez problemu poradziły sobie z wyzwaniem pracy zdalnej. Ich pracownicy otrzymali proste w obsłudze i przyjazne dla użytkowników narzędzia do wymiany

plików, wideokonferencji czy zdalnej kolaboracji na wspólnych dokumentach, bez istotnego zwiększenia zagrożenia dla bezpieczeństwa sieci i bez potrzeby dodatkowych nakładów inwestycyjnych na nową infrastrukturę i dodatkowe licencje.

6. Korzyści chmury wykraczają jednak daleko poza wygodę korzystania z aplikacji biurowych. Przedsiębiorstwa wdrażające chmurę uzyskują dostęp do dynamicznie skalowalnych zasobów obliczeniowych dostawcy, które mogą być wykorzystane m.in. w celu predykcji awarii, prognozowania zużycia i zapotrzebowania, prognozowania cen surowców, prowadzenia badań R&D związanych z analizą big data czy obliczeniami macierzowymi. W większości przypadków korzystanie z prawidłowo wdrożonej chmury pozwoli na obniżenie kosztów systemów IT, zwiększy szybkość i dostęp do danych, poprawi innowacyjność przedsiębiorstwa i poprawi bezpieczeństwo danych.
7. Sektor utilities pozostaje w tyle za innymi mocno regulowanymi sektorami: bankowym i ubezpieczeniowym, farmaceutycznym, telekomunikacyjnym. Wśród przyczyn niskiej adopcji chmury w branży energetycznej wskazuje się na bariery prawne (niepewność prawa i brak dostatecznego uregulowania), wysokie koszty początkowe wdrożenia oraz niski poziom wiedzy w zakresie nowych technologii. W rzeczywistości, realną barierą innowacji okazują się jednak często wewnętrzne obawy organizacji, związane np. z brakiem wystarczającej wiedzy czy obawą przed zmianami. Obawy te nie są w pełni uzasadnione, a prawidłowo przygotowane i zorganizowane wdrożenie powinno skutkować obniżeniem kosztów i zwiększeniem efektywności organizacyjnej, przy jednoczesnym zwiększeniu bezpieczeństwa systemów i poprawie komfortu pracy. W jednym z omówionych w raporcie wdrożeń, proces transformacji organizacji był prowadzony z udziałem pracowników wspierających pozostałe kadry w procesie zmian w charakterze Ambasadorów Zmian.
8. Podstawową zasadą prawa UE zwiększającą pewność prawa użytkowników chmury jest zasada wolnego przepływu danych w granicach UE. Zasada ta obejmuje zarówno dane nieosobowe jak i dane osobowe. Obowiązujące prawo nie zawiera przepisów zakazujących korzystania z chmury w energetyce. Aby jednak w pełni wykorzystać potencjał technologii chmury w polskiej energetyce, kluczowe jest, aby polskie władze wydały dedykowane dla energetyki wytyczne o charakterze technicznym, prawnym i organizacyjnym, usuwające podstawowe wątpliwości uczestników rynku w zakresie związanym z wdrożeniem chmury. Nie ma wątpliwości, że tego typu wytyczne wydane dla sektora finansów przez KNF w 2017 r. i 2020 r. ułatwiają implementację chmury, poprzez zwiększenie pewności i jasności prawa. W ten sam sposób należałoby stymulować adopcję – już coraz bardziej elementarnych – rozwiązań technologicznych w energetyce.



3.

**CZYM JEST CHMURA
OBLICZENIOWA?**

3.1. Definicja; cechy

Cloud computing to w uproszczeniu technologia określająca nowoczesny model przetwarzania danych. Jego głównym założeniem jest udostępnianie zasobów obliczeniowych (infrastruktury, oprogramowania, sprzętu) „na żądanie”. Usługi są dostarczane przy wykorzystaniu serwerów dostawcy, za pomocą Internetu. Zasoby mogą być dynamicznie dostosowywane do potrzeb użytkownika (np. pod względem liczby licencji, mocy obliczeniowej) bez ingerencji usługodawcy. Usługi są zwykle rozliczane w formie regularnych opłat (abonamentu)⁴.

Tradycyjny model pracy zakłada przechowywanie danych w infrastrukturze fizycznej organizacji. Zasoby obliczeniowe są w tym modelu ograniczone możliwościami posiadanego sprzętu, oprogramowania, budżetem oraz zasobami kadrowymi działu IT. Jednak, wraz z rozwojem organizacji, wzrostem potrzeb czy zużyciem sprzętu, konieczna staje się modernizacja infrastruktury. Problemem rozwiązań tradycyjnych jest m.in. wysoki i trudny do oszacowania koszt (nakłady inwestycyjne na kupno sprzętu i oprogramowania, koszty utrzymania i konserwacji). Koszty dostarczenia, wdrożenia, aktualizacji, serwisu i obsługi elementów *software* oraz hardware są zwykle wysokie, a skala rzeczywistego wykorzystania inwestycji niemożliwa lub bardzo trudna do oszacowania przed wdrożeniem. Ponadto rozbudowa infrastruktury wiąże się z koniecznością zwiększenia nakładów na środki zapewniające odpowiedni poziom cyberbezpieczeństwa.

Problemem rozwiązań tradycyjnych jest jednak przede wszystkim brak elastyczności, co szczególnie dotkliwie w energetyce. W razie nagłych zdarzeń (pandemia, klęska żywiołowa powodująca konieczność obsługi setek tysięcy zgłoszeń klientów pozbawionych prądu) organizacja opierająca się o fizyczną infrastrukturę nie ma łatwej możliwości dostosowania się do nowych potrzeb. Organizacja, która w czasach zwykłego zużycia wykorzystuje 70-80% posiadanej mocy obliczeniowej, nie będzie w stanie poradzić sobie z nagłym skokiem w sytuacjach krytycznych. W efekcie, duże spółki, które chcą uniknąć strat związanych z przestojem, decydują się na zakup i utrzymanie infrastruktury fizycznej wielokrotnie przekraczającej ich potrzeby (efekt przeskalowania). To zawyża koszt nakładów inwestycyjnych i zmusza spółki do inwestowania w infrastrukturę, która przez większość czasu nie jest w ogóle wykorzystywana: standardem jest inwestowanie w infrastrukturę, która w codziennej pracy organizacji wykorzystywana jest poniżej 50%⁵.

4 National Institute of Standards and Technology, Definition of Cloud Computing, Special Publication 800-145; GUS: Społeczeństwo informacyjne w Polsce w 2020 r., Warszawa, Szczecin 2020, s. 100.

5 Np. PKO Bank Polski podaje, że infrastruktura IKO pomiędzy lipcem a październikiem 2020 r. zużywała od ok. 20% do ok. 50% mocy zainstalowanej – prezentacja „PKO Bank Polski w czasie pandemii”, s. 7: https://www.pkobp.pl/media_files/0400d803-b511-422d-91ba-39411ae2721d.pdf?fbclid=IwAR0S_-IC2KySbNK-dj8dymKAqxMgFmG-Ljp6fsW7azNfEs9CELeByLWtuk.

W odróżnieniu od infrastruktury fizycznej, zasoby chmury mogą być elastycznie i dynamicznie zmniejszane lub zwiększane według potrzeby (w sposób automatyczny, bez ingerencji użytkownika). Chmura charakteryzuje się **następującymi podstawowymi cechami**⁶:

- a. **skalowalność** – wielkość udostępnianych zasobów jest dostosowana do rzeczywistych i bieżących potrzeb użytkownika;
- b. **multiplatformowość** – usługi chmury pozwalają na dostęp do danych z różnych urządzeń i systemów, często przy pomocy łatwych w obsłudze i intuicyjnych aplikacji znanych dostawców (np. telefonów komórkowych, tabletów, laptopów czy komputerów stacjonarnych);
- c. **elastyczność** – migrację do chmury można ograniczyć do wybranych działów i systemów, a nawet typu danych, w zależności od potrzeb;
- d. **samoobsługowość oraz automatyzacja systemu** – organizacja może zmieniać zakres wykorzystywanych usług samodzielnie, bez konieczności kontaktu z dostawcą;
- e. **dynamiczna alokacja zasobów** - systemy dostawcy automatycznie kontrolują i optymalizują wykorzystanie zasobów.

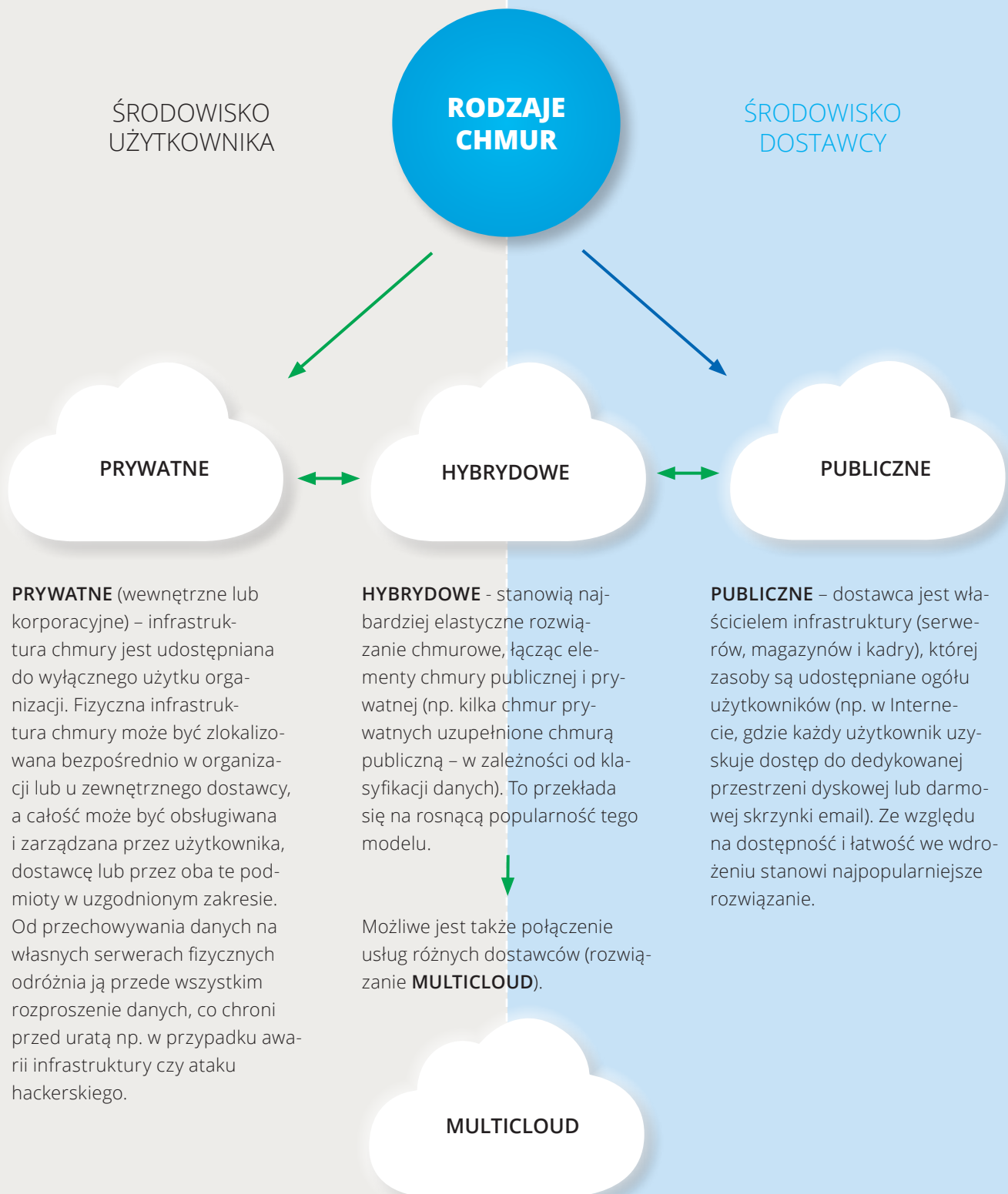
Chmura pozwala więc na *outsourcing* całości lub części wewnętrznych usług IT na dostawców chmurowych świadczących swoje usługi z użyciem Internetu (w tym serwerów, baz danych, sieci, oprogramowania).

Ze względu na dedykowane przeznaczenie chmury dla indywidualnego użytkownika oraz ich dostępność dla nieograniczonej liczby podmiotów wyróżnić można w uproszczeniu następujące **rodzaje**⁷:

6 Peter Mell, Timothy Grance. The NIST Definition of Cloud Computing (Technical report). National Institute of Standards and Technology: U.S. Department of Commerce. doi:10.6028/NIST.SP.800-145. Wrzesień 2011.

7 Robert K. Perrons, How the energy sector could get it wrong with cloud computing, ENERGY EXPLORATION & EXPLOITATION · Volume 33 · Number 2 · 2015 pp. 217–226; Cisco. Cisco Global Cloud Index: Forecast and Methodology, 2016–2021. 2018. str. 22.

RODZAJE CHMUR, DEDYKOWANE PRZEZNACZENIE CHMURY DLA INDYWIDUALNEGO UŻYTKOWNIKA ORAZ ICH DOSTĘPNOŚĆ DLA NIEOGRANICZONEJ LICZBY PODMIOTÓW



PRYWATNE (wewnętrzne lub korporacyjne) – infrastruktura chmury jest udostępniana do wyłącznego użytku organizacji. Fizyczna infrastruktura chmury może być zlokalizowana bezpośrednio w organizacji lub u zewnętrznego dostawcy, a całość może być obsługiwana i zarządzana przez użytkownika, dostawcę lub przez oba te podmioty w uzgodnionym zakresie. Od przechowywania danych na własnych serwerach fizycznych odróżnia ją przede wszystkim rozproszenie danych, co chroni przed uratą np. w przypadku awarii infrastruktury czy ataku hackerskiego.

HYBRYDOWE - stanowią najbardziej elastyczne rozwiązanie chmurowe, łącząc elementy chmury publicznej i prywatnej (np. kilka chmur prywatnych uzupełnione chmurą publiczną – w zależności od klasyfikacji danych). To przekłada się na rosnącą popularność tego modelu.

Możliwe jest także połączenie usług różnych dostawców (rozwiązanie **MULTICLOUD**).

PUBLICZNE – dostawca jest właścicielem infrastruktury (serwerów, magazynów i kadry), której zasoby są udostępniane ogółu użytkowników (np. w Internecie, gdzie każdy użytkownik uzyskuje dostęp do dedykowanej przestrzeni dyskowej lub darmowej skrzynki email). Ze względu na dostępność i łatwość we wdrożeniu stanowi najpopularniejsze rozwiązanie.

Źródło: opracowanie własne

3.2. Przykładowe elementy systemów IT podlegające migracji

Co istotne, wdrożenie chmury obliczeniowej nie wymaga przemodelowania całej istniejącej struktury informatycznej. Wdrożenia odbywają się etapami, a strategia migracji koncentruje na zachowaniu stabilności działalności operacyjnej i optymalizacji zużycia zasobów chmury (zob. rozdział 6).

Możliwe jest przy tym przeniesienie do chmury jedynie niewielkiego wycinku działalności organizacji, w tym nawet najbardziej podstawowych funkcji:

- a. systemu **poczty e-mail, narzędzi biurowych** (edytory tekstu, arkusze kalkulacyjne) i **komunikatorów** – dzięki temu organizacja uzyskuje elastyczny dostęp do kluczowych narzędzi biznesowych z pozycji różnych urzędzeń, zapewniając pracownikom możliwość efektywnej pracy zdalnej, wideokonferencji, kolaboracji nad wspólnymi dokumentami w czasie rzeczywistym, prostej wymiany plików *online*;
- b. **przechowywanie danych**, archiwizacja, kopie zapasowe;
- c. **hosting** strony internetowej i wewnętrznych narzędzi (np. system urlopowy działu HR).

Wdrażanie rozwiązań chmurowych w zakresie podstawowych funkcjonalności i np. rozpoczęcie adopcji od projektów typu *Modern Workplace* stanowi rozsądny krok do oswolenia przedsiębiorstwa z transformacją technologiczną. Wraz ze wzrostem doświadczenia w tworzeniu rozwiązań chmurowych dla chmury organizacja może zdecydować się na migrację kolejnych narzędzi:

- d. **oprogramowania księgowo-finansowego**;
- e. aplikacji do zarządzania relacjami z klientami (**CRM**), planowania zasobów przedsiębiorstwa (**ERP**) i zarządzania dokumentami;
- f. stworzenie dedykowanych aplikacji do obsługi klienta;

- g. magazynów danych pozyskiwanych z różnych sensorów zlokalizowanych w krytycznych miejscach infrastruktury;
- h. rozmaitych aplikacji pozwalających na analizowanie danych przechowywanych, a magazynach danych zlokalizowanych w chmurze.

Chmura pozwala na wykupienie zasobów obliczeniowych niezbędnych **w działaniach R&D, analizie big data i wykonywaniu obliczeń macierzowych**, kluczowych dla prognozowania zapotrzebowania i zużycia, cen surowców czy predykcji awarii. Uzyskując możliwość elastycznego wykupywania zasobów do konkretnych projektów badawczych, organizacje mogą zwiększyć swoją innowacyjność i zyskać długoterminowo.

Wreszcie chmura stanowi konieczny fundament dla wdrażania i rozwoju dalszych cyfrowych innowacji, kluczowych dla branży energetycznej, jak wykorzystywanie i obsługiwanie rozwiązań opartych o **Internet Rzeczy** (*Internet of Things*, IoT) czy wdrażanie **sztucznej inteligencji** (*artificial intelligence*, AI) np. w celu zmodernizowania platform obsługi klienta.

A nighttime photograph of the New York City skyline. The Freedom Tower is the central focus, illuminated against a dark, cloudy sky. The Manhattan Bridge is visible in the foreground, with its stone towers and suspension cables. Other skyscrapers are visible in the background, some with lights on. The overall color palette is dominated by blues and greys, with some warm lights from the buildings.

4.

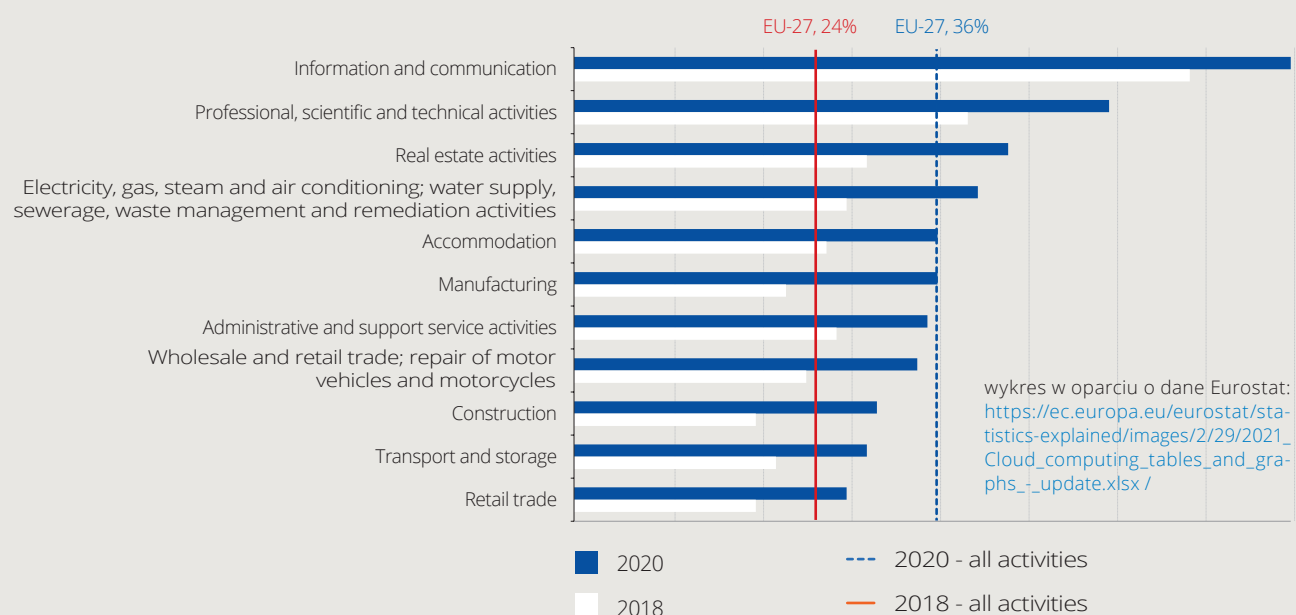
ŚWIATOWE TRENDY

4.1. Wykorzystanie chmury w sektorze prywatnym

Adopcja chmury w Europie i Polsce pozostaje na niskim poziomie, a spółki, które zdecydują się na wdrożenie rozwiązań chmury mogą liczyć na uzyskanie pewnej przewagi konkurencyjnej, wynikającej z niskiej adopcji technologii przez konkurentów. Dostrzegalne są jednak trendy wzrostowe. W 2020 r. 36% przedsiębiorstw działających na terenie Unii Europejskiej korzystało z rozwiązań chmurowych, co stanowi wzrost o 10 p. procentowych w porównaniu do poziomu z 2018 r. (26%). Większość organizacji korzysta z chmury w podstawowym zakresie: 76% przedsiębiorców wykorzystuje chmurę do obsługi poczty elektronicznej, 67% do przechowywania plików. Nieco ponad połowa (55%) korzysta z zaawansowanych usług chmurowych związanych z np. aplikacjami finansowo-księgowymi, zarządzaniem relacjami z klientami lub wykorzystaniem mocy obliczeniowej do uruchamiania aplikacji biznesowych⁸.

Na poziomie Unii Europejskiej, liderami korzystania z chmury jest sektor IT i komunikacji (ponad 70% przedsiębiorstw sektora wykorzystuje chmurę). Wykorzystanie w sektorze utilities, w tym energii elektrycznej i gazu, osiągnęło w 2020 r. poziom 40%:

USE OF CLOUD COMPUTING SERVICES, BY ECONOMIC ACTIVITY, EU-27, 2018 AND 2020 (% OF ENTERPRISES)



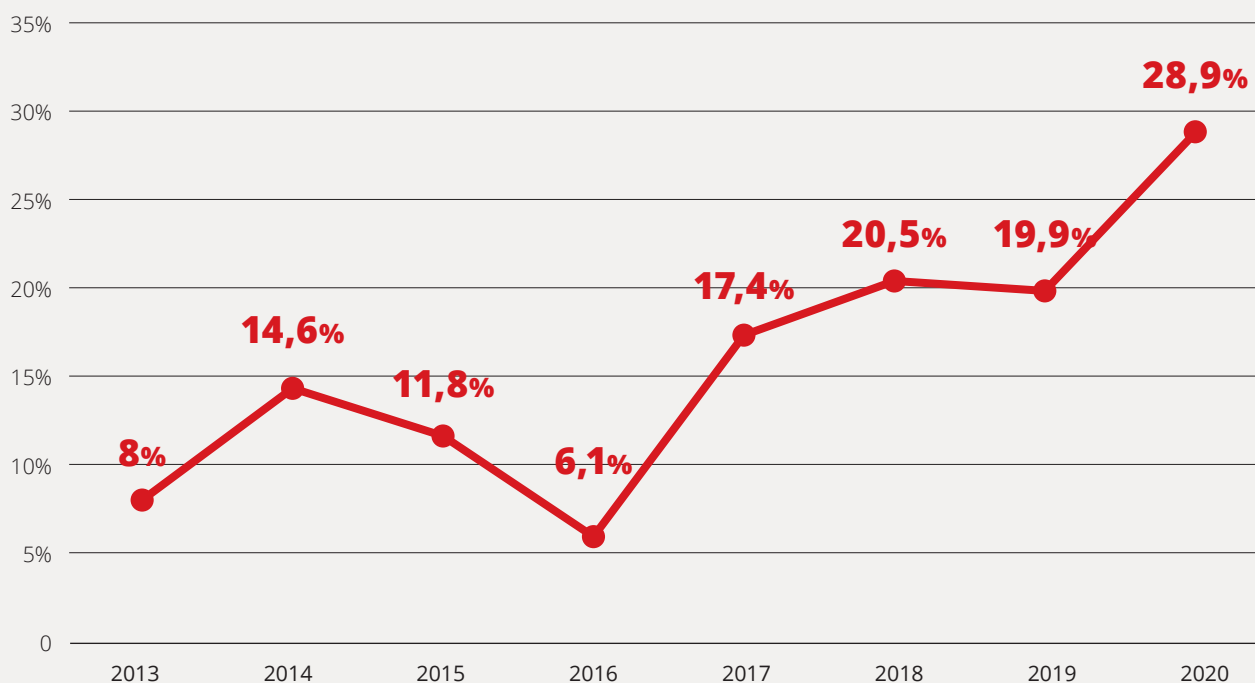
8 Opracowanie własne na podstawie danych Eurostat.



Polska pozostaje w tyle UE jeśli chodzi o adopcję chmury, zajmując 23 miejsce za m.in. Czechami, Słowacją, Węgrami. Według danych Eurostat, wykorzystanie chmury w Polsce w 2018 r. raportowało jedynie 11% przedsiębiorców. W 2019 r. było to 17,5% przedsiębiorców, a w 2020 r. 24,4%. Porównanie z liderami rankingu, krajami skandynawskimi, wypada pesymistycznie: ponad 75% przedsiębiorców w Finlandii, 70% w Szwecji i 67% w Danii raportuje wykorzystanie chmury w biznesie.

Analogicznie do rynku europejskiego, również polski rynek charakteryzuje się zauważalnym rozwarstwieniem poziomu adopcji chmury w zależności od branży. Największe zainteresowanie wykazują przedsiębiorcy z sektora informacji i komunikacji oraz działalność profesjonalna, naukowa i techniczna. Adopcja chmury przez działające w Polsce *utilities*⁹ pozostaje na niskim poziomie. Sektor *utilities* pozostaje w tyle za innymi mocno regulowanymi sektorami: bankowym i ubezpieczeniowym, farmaceutycznym, telekomunikacyjnym¹⁰. Zauważalny jest jednak trend wzrostowy, w efekcie czego już prawie co trzeci przedsiębiorca *utilities* w Polsce korzysta z chmury:

KOLEJNE LATA ADOPCJI - PORÓWNANIE ¹¹



9 Przedsiębiorcy zajmujący się wytwarzaniem lub zaopatrywaniem w energię elektryczną, gaz, parę wodną lub gorącą wodę.

10 Chmura obliczeniowa w sektorze bankowym na świecie, w Europie i w Polsce, Accenture, Warszawa, Kwiecień 2020.

11 Opracowanie własne na podstawie danych GUS (raporty „Społeczeństwo informacyjne w Polsce”).

Jeśli chodzi o strukturę celów użycia w Polsce, wśród dużych przedsiębiorców dominuje wykorzystanie chmury na potrzeby biurowe: 46,8% dużych przedsiębiorców wykorzystuje chmurę do obsługi poczty email, 47,4% do oprogramowania biurowego (dokumenty tekstowe, arkusze kalkulacyjne), 43% do przechowywania plików i 26,7% jako hosting bazy danych.

W naszej ocenie, wykorzystanie chmury w Polsce w sektorze prywatnym, w tym utilities, powinno wzrastać w kolejnych latach wraz z:

- a. przedłużającą się niepewnością pandemiczną i potrzebą zapewnienia gotowości operacyjnej organizacji w razie kolejnego lockdownu lub zmiany trendów pracy na pracę zdalną;
- b. spadkiem kosztów chmury w porównaniu do kosztów infrastruktury fizycznej (koszty serwerów (sprzętu), koszty pracownicze, koszty powierzchni biurowych i licencji oprogramowania, koszty usług IT, koszty zapewnienia cyberbezpieczeństwa);
- c. ustabilizowaniem sytuacji prawnej w sektorach regulowanych (za sprawą wytycznych regulatorów) i w zakresie danych osobowych;
- d. rosnącym zagrożeniem cyberataków na infrastrukturę przedsiębiorstw energetycznych.

4.2. Chmura a państwowe strategie cyfryzacji i cyberbezpieczeństwa

Co szczególnie ważne dla sektora energetyki jako sektora poddanego silnym regulacjom prawnym, w którym państwo wciąż odgrywa znaczącą rolę, korzystanie z chmury wpisuje się w europejskie i krajowe strategie w cyfryzacji i cyberbezpieczeństwa.

4.2.1. Działania na poziomie europejskim

Zapewnienie bezpieczeństwa przetwarzania danych w chmurze obliczeniowej i jej upowszechnienie stanowi jeden z elementów strategii rozwoju Unii Europejskiej. W 2012 r. Komisja UE opublikowała „Europejską strategię w zakresie chmur obliczeniowych” zapowiadającą opracowanie standardów mających zwiększyć wykorzystanie chmury obliczeniowej we wszystkich sektorach gospodarki. Efektem Strategii było m.in. częściowe ustandaryzowanie postanowień umownych w zakresie SLA (*Service Level Agreements*)¹², zainicjowanie projektu *Cloud-for-Europe* (C4E)¹³ udzielającego wsparcia władzom publicznym w nabywaniu produktów i usług w chmu-

12 <https://ec.europa.eu/digital-single-market/en/news/cloud-and-edge-computing-different-way-using-it-brochure>

13 <https://ec.europa.eu/digital-single-market/en/news/cloud-europe-stage>

rze oraz ustanowienie Europejskiego partnerstwa na rzecz chmury obliczeniowej (European Cloud Partnership - ECP) – grupy doradczej mającej wyznaczać kierunki rozwoju chmury w UE¹⁴.

Wnioski z pracy ECP w postaci zaleceń Rady Sterującej znalazły odzwierciedlenie m.in. w strategii jednolitego rynku cyfrowego. W ramach jej realizacji 16 kwietnia 2016 r. Komisja opublikowała pakiet środków służących cyfryzacji przemysłu europejskiego, w tym komunikat w sprawie „Europejskiej inicjatywy w zakresie przetwarzania w chmurze”, powołujący inicjatywę *The European Open Science Cloud* (EOSC). Celem EOSC jest stworzenie zaufanego środowiska do przechowywania, udostępniania, przetwarzania danych naukowych (takich jak publikacje, dane i oprogramowanie)¹⁵.

Istotnym krokiem było zapewnienie swobodnego i bezpiecznego przesyłu danych w obrębie UE w oparciu o zasadę wolnego przepływu danych w granicach Wspólnoty. Ogólne rozporządzenie o ochronie danych z roku 2016 r. („**RODO**”¹⁶) przewidywało swobodny przepływ danych osobowych. Jednakże dopiero rozporządzenie z dnia 14 listopada 2018 r.¹⁷, w sprawie ram swobodnego przepływu danych nieosobowych w UE zakazało ograniczania przepływu danych nieosobowych między państwami członkowskimi i systemami informatycznymi w Europie. Przedmiotowe rozporządzenie wraz z RODO i uzupełniane przez wytyczne Komisji¹⁸ zawierające wskazania co do przetwarzania tzw. „zbiorów mieszanych” zapewnia kompleksowe i spójne podejście do w pełni swobodnego przepływu danych w UE (zob. rozdział 5.2.1).

Na poziomie Unii Europejskiej trwają prace nad regulacją w zakresie cyberbezpieczeństwa dotyczącą chmury obliczeniowej. 19 lutego 2020 r. Komisja (UE) opublikowała komunikat zawierający „Europejską strategię w zakresie danych”¹⁹, zapowiadającą m.in. zliberalizowanie rozwiązań prawnych ograniczających pełne wykorzystanie potencjału chmury. W komunikacie zapowiedziano również prace nad europejską federacją „energooszczędnej i godnej zaufania infrastruktury chmurowej”. Projekt miałby uwzględnić „szczególne potrzeby przemysłu w UE, w tym hybrydowe modele wdrażania chmury obliczeniowej, które pozwalają na przetwarzanie danych na obrzeżach sieci bez opóźnienia (tzw. *cloud-to-edge*)”.

W październiku 2020 r. 25 państw członkowskich UE, w tym Polska, podpisało deklarację rozwoju usług chmurowych dla administracji publicznej i sektora prywatnego. W ten sposób wyrażono wolę podjęcia współpracy

14 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Unleashing the Potential of Cloud Computing in Europe; Trusted Cloud Europe Survey - Assessment of Survey Responses, Brussels 15.07.2014.

15 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, European Cloud Initiative -Building a competitive data and knowledge economy in Europe, Brussels, 19.4.2016

16 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE

17 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej

18 Komunikat Komisji Europejskiej do Parlamentu Europejskiego, Rady, Wytyczne dotyczące rozporządzenia w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej, Bruksela, dnia 29.5.2019 r., COM(2019) 250 final

19 Komunikat Komisji Europejskiej do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Europejska strategia w zakresie danych, Bruksela, dnia 19 lutego 2020 r., COM(2020) 66.

w celu powołana do życia Europejskiej Federacji Chmur, której celem ma być ukształtowanie bezpiecznych, energooszczędnych i interoperacyjnych usług chmurowych nowej generacji. W ramach wykonania powyższych założeń państwa zadeklarowały opracowanie Europejskiego Podręcznika dla Usług Chmurowych (*Cloud Rulebook*), stanowiącego zestaw technicznych zasad, standardów i norm dla chmury oraz uruchomienie europejskich platform (*marketplaces*), na których dostawcy mogliby oferować swoje usługi²⁰.

Równolegle, Europejska Agencja ds. Bezpieczeństwa Cybernetycznego (ENISA) z inicjatywy Komisji UE pracuje nad stworzeniem jednolitego europejskiego systemu certyfikacji w zakresie bezpieczeństwa cybernetycznego usług w chmurze. Inicjatywa ma stanowić odpowiedź na brak zaufania użytkowników do dostawców usług, który wynika po części ze znacznego rozdrobnienia rynku usług chmurowych²¹. Jednostką wsparcia rozwoju cyfrowego jest również powołany do życia w 2021 r. Europejski sojusz na rzecz danych przemysłowych, chmury i urządzeń brzegowych (*European Alliance for industrial data, cloud and edge*), który ma zrzeszać państwa członkowskie, dostawców chmury, użytkowników chmury z różnych sektorów oraz zainteresowane strony ze środowiska akademickiego i społeczeństwa obywatelskiego. Celem sojuszu jest ułatwienie powstania europejskiej oferty nowej generacji, godnych zaufania, energooszczędnych i konkurencyjnych usług chmurowych i brzegowych²².

Na uwagę zasługują również podejmowane przez ustawodawcę europejskiego i krajowego kroki w zakresie regulacji cyberbezpieczeństwa, potwierdzające rosnące znaczenie cyberbezpieczeństwa dla stabilności gospodarki i bezpieczeństwa państw członkowskich UE. 6 lipca 2016 r. wdrożona została dyrektywa NIS²³ (*Network and Information Systems Directive*) stanowiąca pierwszy akt prawny UE w zakresie cyberbezpieczeństwa. Dyrektywa miała gwarantować wysoki poziom cyberbezpieczeństwa, m.in. poprzez nałożenie szeregu obowiązków na operatorów usług kluczowych (w tym w energetyce) i dostawców usług cyfrowych (w tym dostawców usług chmurowych), np. w zakresie zgłaszania incydentów bezpieczeństwa. Dyrektywa została implementowana do polskiego porządku prawnego ustawą o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 r.²⁴ Aktualnie trwają również prace nad nowelizacją ustawy, która ma przyczynić się do „uszczelnienia” krajowego systemu cyberbezpieczeństwa²⁵.

16 grudnia 2020 r. Komisja Europejska opublikowała również projekt nowej strategii cyberbezpieczeństwa dla Unii Europejskiej, w skład której wchodzi m.in. nowa propozycja dyrektywy dotyczącej środków na rzecz wysokiego poziomu bezpieczeństwa sieci i systemów komunikacji na terytorium Unii (tzw. dyrektywa NIS 2)²⁶.

20 <https://www.gov.pl/web/cyfryzacja/polska-bedzie-wspoltworzyc-europejska-federacje-chmur>

21 <https://ec.europa.eu/digital-single-market/en/news/towards-more-secure-and-trusted-cloud-europe>

22 <https://ec.europa.eu/digital-single-market/en/news/cloud-and-edge-computing-different-way-using-it-brochure>

23 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194 z 19.07.2016.).

24 Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560).

25 Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych z dnia 8 września 2020 r.

26 Wniosek Dyrektywa Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylająca dyrektywę (UE) 2016/1148, Bruksela, dnia 16.12.2020 r., COM(2020) 823 final

Projekt przewiduje zaostrzenie wymogów w zakresie bezpieczeństwa i sprawozdawczości oraz implementowanie rygorystycznych środków nadzoru ze strony krajowych organów. Wprowadza również m.in. nowe mechanizmy współpracy międzynarodowej i zwiększa rolę ENISA. Projektowane zmiany mają wymusić wyższe standardy cyberbezpieczeństwa. W strategii znalazł się również projekt nowej dyrektywy w sprawie odporności podmiotów krytycznych²⁷ (*resilience of critical entities*), która rozszerza i pogłębia zakres dyrektywy w sprawie europejskiej infrastruktury krytycznej z 2008 r.

4.2.2. Działania władz polskich

Pewne działania przygotowujące rynek (w tym administrację publiczną) do wdrożenia chmury podejmuje również polski rząd. W Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024²⁸ stanowiącej również realizację założeń dyrektywy NIS, Rada Ministrów podkreśliła znaczenie chmury obliczeniowej dla podnoszenia krajowego systemu cyberbezpieczeństwa:

„Rząd w ramach współpracy administracji rządowej z administracją samorządową będzie rekomendował i działał na rzecz jednostek samorządu terytorialnego w zakresie podnoszenia kompetencji w projektowaniu procesów zwiększających cyberbezpieczeństwo, w szczególności: w doborze, wdrażaniu i utrzymaniu środków technicznych zwiększających cyberbezpieczeństwo, w tym korzystania z nowoczesnych i bezpiecznych modeli przetwarzania w chmurach obliczeniowych [...]”²⁹

Rada Ministrów, jako realizację jednego z celów Strategii, zapowiedziała także opracowanie Narodowych Standardów Cyberbezpieczeństwa określających wymogi organizacyjne i techniczne dot. bezpieczeństwa modeli chmury obliczeniowej³⁰.

Równoległym krokiem mającym na celu uregulowanie zagadnienia chmur obliczeniowych było przejście dnia 24 września 2019 r. przez Radę Ministrów uchwały w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa” (WIIP)³¹. Celem uchwały jest wprowadzenie do powszechnego stosowania nowych pojęć związanych z wykorzystaniem chmury obliczeniowej w sektorze finansów publicznych. Program WIIP zakłada optymalizację istniejących zasobów teleinformatycznych i aplikacji w sektorze finansów publicznych poprzez dostarczenie nowoczesnych i optymalnych kosztowo technologii informatycznych.

W ramach zbioru Narodowych Standardów Cyberbezpieczeństwa, w lutym 2020 r. opublikowano *Standardy Cyberbezpieczeństwa Chmur Obliczeniowych*³². Standardy stanowią zbiór wymagań prawnych, organizacyjnych

27 Wniosek Dyrektywa Parlamentu Europejskiego i Rady sprawie odporności podmiotów krytycznych, Bruksela, dnia 16.12.2020 r., COM(2020) 829 final

28 Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r., Monitor Polski, poz. 1037.

29 Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r., Monitor Polski, poz. 1037, s. 11.

30 Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r., Monitor Polski, poz. 1037, s. 15.

31 Uchwała nr 97 Rady Ministrów z dnia 11 września 2019 r., Monitor Polski, poz. 862.

32 Narodowe Standardy Cyberbezpieczeństwa, Standardy Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO), v. 1.00 – luty 2020 - zob. <https://chmura.gov.pl/informacje/scco/>.

i technicznych, mających na celu stworzenie jednolitych standardów bezpieczeństwa, umożliwiających migrację systemów i danych do modelu przetwarzania w chmurze obliczeniowej. Celem SCCO jest podniesienie poziomu odporności systemów IT administracji publicznej i sektora prywatnego i zdolności do zapobiegania i reagowania na incydenty cyberbezpieczeństwa. Standardy skierowano m.in. do dostawców usług chmur obliczeniowych oferujących usługi w publicznej chmurze obliczeniowej.

Działania polskiego rządu, choć dotychczas nakierowane przede wszystkim na wykorzystanie chmury w administracji, stabilizują nieco krajobraz regulacyjny, dając wyraźny sygnał, że ustawodawca akceptuje istnienie chmury obliczeniowej i wspiera jej implementację.

Podobnych sygnałów wciąż brakuje w energetyce. Dla porównania, sektor finansów może opierać wdrożenia chmury na wytycznych wydanych przez UKNF w zakresie przetwarzania informacji w chmurze przez podmioty nadzorowane³³. Wytyczne określają model referencyjny stosowania usług chmury m.in. w zakresie szacowania ryzyka, minimalnych wymagań technicznych i organizacyjnych usługi, wymagań w zakresie formy i treści umowy z dostawcą usług czy wymagań zgodności z normami, jakie spełniać musi wybrany dostawca. Choć wytyczne podlegają stosowaniu bez uszczerbku dla przepisów prawa, to jednak zapewniają pewien stopień przejrzystości wymogów regulacyjnych i tego, jak UKNF będzie je egzekwował. Tym samym, ułatwiają podmiotom nadzorowanym implementację innowacyjnych rozwiązań chmury obliczeniowej.

Na polskim rynku dostrzegalne są również prywatne inicjatywy popularyzujące chmurę obliczeniową. W 2018 r., z inicjatywy PKO Banku Polskiego S.A. i Państwowego Funduszu Rozwoju w ramach strategii „Wspieramy rozwój Polski i Polaków” powołano spółkę technologiczną, Operator Chmury Krajowej sp. z o.o., mającą być największym krajowym dostawcą usług chmurowych³⁴. Celem Chmury Krajowej jest „przyspieszenie cyfrowej transformacji polskich przedsiębiorstw oraz instytucji publicznych”³⁵. Powodzenie projektu ma zapewnić wsparcie największych dostawców rozwiązań chmurowych: Google i Microsoft.

4.3. Wdrożenie chmury obliczeniowej w wybranych organizacjach *(case studies)*

Po rozwiązaniu chmurowe zaczynają sięgać przedsiębiorstwa funkcjonujące na rynkach regulowanych, krajowe i zagraniczne spółki energetyczne, spółki i organizacje powiązane ze skarbem państwa. Analiza przykładowych

33 Komunikat Urzędu Komisji Nadzoru Finansowego dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej z dnia 23 stycznia 2020 r., który zastąpił komunikat z 23 października 2017 r. dotyczący „korzystania przez podmioty nadzorowane z usług przetwarzania danych w chmurze obliczeniowej”. Aktualne wytyczne stanowią więc wieloletnie doświadczenie UKNF w zakresie wdrożeń chmurowych.

34 <https://media.pkobp.pl/70946-operator-chmury-krajowej-rozpoczal-dzialalnosc-operacyjna-pko-bank-polski-zostal-pierwszym-klientem>; <https://wgospodarce.pl/informacje/79202-chmura-krajowa-czym-bedzie-i-co-zmieni>

35 <https://chmurakrajowa.pl/dlaczego-chmura-krajowa/>

wdrożeń pomaga zrozumieć najistotniejsze korzyści związane z tą technologią, które wykorzystać mógłby sektor energetyki.

Grupa Tauron³⁶ – jest zdecydowanym pionierem na polskim rynku energetycznym w zakresie wdrożeń chmurowych. Wdrożenie chmury rozpoczęto w 2019 r. a pierwszym krokiem była modernizacja infrastruktury sieciowej i implementacja chmurowego pakietu Microsoft Office 365. Wdrożenie okazało się sukcesem. Po wybuchu pandemii zarząd spółki zdecydował o skierowaniu pracowników biurowych do pracy zdalnej i tu rozwiązania chmurowe okazały się nieocenione. Pracownicy uzyskali dostęp do szybkich, sprawnych i prostych w obsłudze aplikacji biurowych Office 365, dostępnych z pozycji różnych urzędzeń (również mobilnie). Jak ocenia CIO Grupy:

„Gdybyśmy tego nie zrobili w roku 2019, nie byłibyśmy w stanie tak sprawnie funkcjonować w okresie obostrzeń wprowadzonych w czasie epidemii w marcu i kwietniu br. Dzięki przeprowadzonej transformacji mamy gotową infrastrukturę pozwalającą na jednoczesną, zdalną pracę 11 tys. naszym pracownikom. Do tej pory z pracy z domu korzystało zaledwie kilkaset osób w Grupie TAURON, pomimo że mogli oni korzystać z niej średnio 2 razy w miesiącu. Teraz większość pracowników biurowych robi to pięć dni w tygodniu.”³⁷

Przedstawiciele Grupy deklarują, że zamierzają rozwijać funkcjonalności umożliwiające efektywniejszą i wydajniejszą pracę zdalną oraz skupić się na rozwiązaniach związanych z utrzymaniem systemów IT, zapewnieniem ciągłości ich działania i bezpieczeństwem. W tym celu planowana jest dalsza wirtualizacja istniejącego środowiska i wykorzystanie chmury hybrydowej.

Co więcej, na początku 2020 r. Tauron Wydobycie, w oparciu o chmurę Microsoft, wdrożył unikalny system monitorowania awarii sprzętu w trzech zakładach górniczych. System pozwala na zbieranie w czasie rzeczywistym danych o ewentualnych incydentach, zwiększając szybkość reakcji na zdarzenia i tym samym prowadząc do obniżenia kosztów ewentualnych napraw. Na jego podstawie Tauron Wydobycie tworzy centralną bazę danych o awariach, mającą ułatwić tworzenie analiz w formie graficznej i tabelarycznej w celu lepszego zrozumienia incydentów³⁸.

Grupa LOTOS S.A.³⁹ – na początku 2020 r. w Grupie LOTOS rozpoczęto wdrażanie projektu zwanego „Cyfrowym biurkiem”, polegającego na stopniowej cyfryzacji Grupy i przeniesienie części funkcjonalności do chmury. Pierwszym krokiem jego realizacji było wdrożenie usługi Microsoft 365, w tym Microsoft Teams, którego uruchomienie zbiegło się z wybuchem pandemii i koniecznością dokonania reorganizacji systemu pracy.

Pomimo konieczności szybkiego przeniesienia pracowników w tryb pracy zdalnej wdrożenie miało charakter etapowy. Pełne wykorzystanie poprzedziły działania pilotażowe dla wąskiej grupy kadr – początkowo do

36 <https://itwiz.pl/jaki-sposob-grupa-tauron-dostosowala-sie-funkcjonowania-czasie-epidemii/>

37 Zob. <https://itwiz.pl/jaki-sposob-grupa-tauron-dostosowala-sie-funkcjonowania-czasie-epidemii/>

38 Zob. <https://media.tauron.pl/pr/486246/cyfryzacja-ktora-daje-oszczednosci>

39 Zob. <https://www.kierunekchemia.pl/artukul,80758,chlura-zasila-lotos.html>

wirtualnej rzeczywistości przeniesiono posiedzenia Zarządu Grupy, spotkania komitetu inwestycyjnego i spotkania kadry managerskiej. Następnie pracę zdalną wprowadzono w księgowości i na produkcji i przeprowadzono cykl szkoleń dla prawie 1300 pracowników. Wsparciem było uruchomienie programu Ambasadorów Zmiany – grupy pracowników mających pełnić rolę wsparcia dla pozostałych kadr podczas transformacji.

Działania, pomimo pandemii, umożliwiły dokonanie pełnego wdrożenia dla wszystkich pracowników, którzy mogą w pełni efektywnie pracować z każdego miejsca na świecie, tworzyć cotygodniowe raporty, współdzielić dokumenty i równolegle je edytować. Wdrożenie chmury w podstawowej wymianie informacji jest jedynie początkiem cyfrowej transformacji. Jak deklaruje *Global Chief Information Officer*, Grupa LOTOS.

„LOTOS stopniowo, ale systematycznie przechodzi z firmy bazującej na obiegu papierowym na w pełni zdigitalizowany. Wykorzystujemy cyfrowy podpis i zaawansowaną pracę grupową. Docelowo chcemy, by całe życie naszych dokumentów było tylko życiem cyfrowym. Sam projekt zaczynał się dość niewinnie jednak szybko zauważyliśmy olbrzymią ilość zależności i wzajemnych powiązań między jego poszczególnymi elementami oraz wykorzystywanymi technologiami. Na szczęście ze wsparciem MCS udało się szybko opracować profesjonalną road mapę wdrożenia M365 wraz ze wszystkimi zależnymi elementami. Zrobiliśmy to w samą porę i okazało się strzałem dziesiątkę.”⁴⁰

Priorytetem Grupy LOTOS podczas wdrożenia chmury stanowiło zapewnienie bezpieczeństwa danych. Wraz z usługą *Azure Information Protection* spółka wprowadziła system etykietowania i monitorowania dokumentów. Dane są nie tylko szyfrowane, a zarządzanie kluczem szyfrowania pozostaje po stronie Grupy, ale również spółka ma pełny wgląd w ścieżkę przepływu i edycji dokumentów, dzięki czemu posiada dostęp do bieżących informacji o tym kto je otwiera i z jakiej lokalizacji, ale również może elastycznie zarządzać dostęпами do dokumentów zawierających np. dane wrażliwe.

General Electric Power⁴¹ jest jednym ze światowych liderów w dziedzinie energetyki, dostarczając technologie, rozwiązania i usługi w całym łańcuchu dostaw energii, od wytwarzania do zużycia, zasilając ponad jedną trzecią świata. GE wykorzystuje chmurę jako podstawową infrastrukturę przetwarzania danych: m.in. do zbierania i przetwarzania danych z 20 miliardów sensorów w ponad 900 placówkach klientów na całym świecie i przesyłania ponad 500.000 wpisów na sekundę. Zebrane dane są przechowywane w chmurze i dostępne dla wszystkich uprawnionych użytkowników, niezależnie od położenia, w tym analityków lub klientów GE.

GE wykorzystuje ponadto technologię chmurową do procesów predykcji i zarządzania wydajnością. System automatycznie wysyła powiadomienia do klientów, gdy wykryte zostaną jakiegokolwiek problemy ze sprzętem lub odstępstwa od zakładanych norm.

40 Zob. <https://www.kierunekchemia.pl/arttykul,80758,chlura-zasila-lotos.html>

41 Zob. <https://aws.amazon.com/solutions/case-studies/ge-power/>

Jakie są korzyści z wdrożenia chmury?

- zwiększenie transferu danych;
- **automatyzacja** – dane z zainstalowanych czujników przesyłane są bezobsługowo;
- **szybkość reagowania** – chmura pozwala pracownikom elektrowni na dostęp do danych w czasie rzeczywistym i bieżące podejmowanie decyzji dotyczących obsługi i zarządzania infrastrukturą fizyczną. To zwiększa nie tylko trafność podejmowanych decyzji, ale również prędkość reagowania na potencjalne usterki, zmniejszając potencjalne straty z tym związane;
- **lepsza jakość obsługi i zarządzania** – zwiększona ilość przetwarzanych danych przekłada się na głębszy i szybszy wgląd w pracę systemów zarządzającymi elektrowniami. GE Power otrzymuje dokładniejszą analizę warunków panujących w danym zakładzie i prawdopodobieństwo ich wpływu na sprzęt (możliwość predykcji zużycia poszczególnych części i sprzętu). W rezultacie, GE może odpowiednio zaplanować konserwację czy wymianę, minimalizując tym samym ewentualne przestoje i dodatkowe koszty związane z niespodziewaną awarią systemu.

innogy Czech⁴² to europejska firma energetyczna, która dostarcza gaz, energię elektryczną i inne usługi dla 1,6 miliona klientów w Czechach, obsługuje 65 000 km sieci elektrycznych, zarządza sześcioma podziemnymi magazynami gazu o łącznej pojemności 2,7 miliarda metrów sześciennych oraz produkuje ciepło i energię elektryczną w 18 zakładach.

innogy Czech podjęła decyzję o wdrożeniu chmury, gdy wskutek powodzi została zmuszona do zamknięcia centrum danych w Brnie. Zespół IT firmy dostrzegł w tym okazję do zmiany strategii IT spółki poprzez przejście do chmury, w celu zwiększenia elastyczności i efektywności zarządzania infrastrukturą IT. Do tej pory, spółka polegała na wewnętrznych systemach SAP i aplikacjach dedykowanych dla branży energetycznej. Innogy przeniosło do chmury całe oprogramowanie SAP (wariant SAP IS-U) i CRM. innogy Czech mogła także skorzystać na konwersji nakładów inwestycyjnych na infrastrukturę IT (CAPEX) na wydatki operacyjne uiszczane dostawcy chmury. Co ważne, proces wdrożenia następował powoli i etapowo, tak, aby zapewnić stabilność biznesu.

Jakie są korzyści z wdrożenia chmury?

- **bezpieczeństwo** – dotychczasowe systemy innogy Czech zostały zaprojektowane tak, aby były szeroko dostępne. Opierając się na rozwiązaniu chmurowym, zespół IT był w stanie wesprzeć te cele, budując

42 Zob. <https://aws.amazon.com/solutions/case-studies/innogy/>

stabilne, redundantne i szyfrowane połączenie pomiędzy istniejącym centrum danych a chmurą. Użytkownicy mogą uzyskać dostęp do wysoce dostępnego systemu w chmurze z poziomu bezpieczeństwa sieci korporacyjnej;

- **redukcja ilości danych** – firma zmniejszyła produkcyjną bazę danych SAP IS-U o 30%;
- **oszczędność** - elastyczność chmury pozwala innogy Czech płacić tylko za zużywane zasoby obliczeniowe i magazynowe. Dzięki przejrzystości kosztów i użytkowania, może natychmiast sprawdzić zużycie usług i efektywniej zarządzać tymi zasobami (innogy Czech oszacowało, że zasoby obliczeniowe w chmurze kosztowały ich o 20% mniej niż potencjalne wdrożenia lokalne);
- **innowacyjność** – innogy Czech usprawniła proces zarządzania zmianami, umożliwiając szybkie uruchomienie nowego oprogramowania i zasobów. Ponieważ posiadane systemy nie są już używane do obsługi systemów SAP, usługi biznesowe odczuwalnie przyspieszyły. W rezultacie technologia jest obecnie czynnikiem umożliwiającym innowacje biznesowe, a nie blokującym je.

Shell⁴³ - w 2012 r. rozszerzył *outsourcing* centrów danych o usługi chmury, pozwalające na zdalny dostęp do danych bez konieczności utrzymywania własnych serwerów. Firma wykorzystuje rozwiązania chmurowe w zarządzaniu i analizowaniu ogromnych ilości danych geologicznych wytwarzanych przez czujniki sejsmiczne umożliwiające wykrywanie i wydobywanie ropy. Pracownicy Shell Oil używają chmury do analiz, sami zapewniają moc obliczeniową, a następnie uruchamiają modele analityczne na zasadzie płatności za faktyczne użycie.

Za pomocą chmury Shell zwiększył również bezpieczeństwo danych i uzyskał możliwość dokonywania ich historycznych analiz, pozwalających na predykcję incydentów i luk w zabezpieczeniach.

43 Zob. <https://www.computerworld.com/article/2502623/shell-oil-targets-hybrid-cloud-as-fix-for-energy-saving--agile-it.html>; <https://aws.amazon.com/solutions/case-studies/royal-dutch-shell/>

Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej⁴⁴ – jest podmiotem publicznym przyznającym dofinansowania w ramach projektów wspierających ochronę środowiska (np. w ramach walki ze smogiem, wytwarzaniem energii z odnawialnych źródeł energii). NFOŚ zdecydował o wdrożeniu chmury dla *zoptimalizowania* procesów obsługi wniosków o dofinansowania. Do chmury przeniesiono część procesów w kilku najważniejszych obszarach działalności, w tym m.in. programy „Mój Prąd” oraz „Czyste Powietrze”. Stworzono np. możliwość wnioskowania *on-line* poprzez stronę internetową lub zbudowany w chmurze Generator Wniosków o Dofinansowanie, pozwalający na autoryzację z wykorzystaniem Profilu Zaufanego. Zdygitalizowano również proces obiegu i przetwarzania dokumentów oraz przeniesiono oprogramowanie wspomagające zarządzanie SAP.

Kluczowe korzyści związane z wdrożeniem chmury:

- większa wydajność procesów, przyspieszone rozpatrywanie wniosków i wypłat
- dostęp do bieżących danych co do skali wniosków i ich statusów
- stworzenie jednorodnego środowiska informatycznego
- ograniczenie wydatków na infrastrukturę o 2.540.000 zł
- umożliwienie bezpiecznej pracy zdalnej pracowników
- zmniejszenie całkowite kosztów jakie trzeba byłoby wydać na utrzymanie jednorodnego środowiska informatycznego o 1.544.000 zł i zapewnienie narzędzi do codziennej biurowej pracy dla pracowników NFO-ŚiGW.

PKO Bank Polski S.A. jest prekursorem chmurowej rewolucji w Polsce. W 2019 roku bank przyjął strategię cyfryzacji „Road to Cloud”⁴⁵, założeniem której jest przeniesienie najważniejszych systemów IT banku do chmury hybrydowej w ciągu 3 lat⁴⁶. PKO BP rozpoczęło migrację systemów wewnętrznych i stworzyło 11 tysięcy wirtualnych stanowisk dla pracowników.⁴⁷

44 Zob. <https://news.microsoft.com/pl-pl/2020/10/13/programy-realizowane-w-nfosigw-w-oparciu-o-microsoft-azure-wspieraja-ochrone-srodowiska/>; <https://insidecee.pl/narodowy-fundusz-ochrony-srodowiska-i-gospodarki-wodnej-przeniosl-oprogramowanie-do-chmury-microsoft-azure/>

45 Zob. <https://gsmonline.pl/artykuly/pko-bp-chmura-krajowa-projekt-road-to-cloud>

46 Zob. <https://www.pb.pl/pko-bp-najpозniej-za-3-lata-najwazniejsze-systemy-it-w-chmurze-990481>

47 Zob. <https://300gospodarka.pl/wywiady/megaprojekty-chmur-obliczeniowych-google-i-microsoft-w-polsce-wiceprezes-pko-bp-wyjasnia-jak-beda-dzialac>

Przyjęte rozwiązania z powodzeniem zdały egzamin w pandemii. Chmura umożliwiła szybkie stworzenie systemu wideo konsultanta, pozwalając obsłużyć wnioski składane w ramach tarczy finansowej. 450 wideo konsultantów banku mogło w nieprzerwany sposób prowadzić rozmowy wideo z klientami i sprzedawać produkty bankowe małym i średnim przedsiębiorcom. Bank przeniósł również kilkanaście tysięcy pracowników do pracy zdalnej. Rozwiązanie okazało się na tyle zadowalające, że bank planuje pozostawić część z kadr w trybie zdalnym nawet po ustaniu zagrożenia epidemicznego.

Agencja Restrukturyzacji i Modernizacji Rolnictwa⁴⁸ – wdrożenie chmury przez ARiMR stanowi przykład błyskawicznego reagowania na wyzwania pandemii i nowoczesnego podejścia do cyberbezpieczeństwa. Po ogłoszeniu *lockdownu* i zamrożenia gospodarki, ARiMR mogła w nieprzerwany sposób świadczyć wsparcie na rzecz rolników, pomimo skierowania do pracy zdalnej 10 tys. pracowników.

Dzięki wdrożonym rozwiązaniom chmurowym, pracownicy ARiMR pracujący zdalnie mogą w bezpiecznym środowisku IT organizować zdalne spotkania, współtworzyć kanały projektowe czy wymieniać dane. ARiMR wykorzystuje chmurowe komunikatory wideo we własnej działalności edukacyjnej: w ten sposób przeprowadzono już ok. 280 tysięcy szkoleń dla różnych grup użytkowników końcowych, administratorów, pracowników działu wsparcia, czy też doradców, urzędów i innych instytucji współpracujących.

48 Zob. <https://news.microsoft.com/pl-pl/2020/12/18/zdalne-sztaby-kryzysowe-agencji-restrukturyzacji-i-modernizacji-rolnictwa-w-chmurze-microsoft/>



5.

POLSKA ENERGETYKA W CHMURZE

5.1. Wstęp; specyfika sektora energetyki

Historycznie sektor energetyki podchodził do nowych technologii raczej ostrożnie, a przyczyn takiego podejścia może być wiele. Energetyka ma kluczowe znaczenie dla bezpieczeństwa państwa i porządku publicznego, stanowiąc infrastrukturę krytyczną. Nawet stosunkowo krótkie przerwy w dostawie prądu mogą zagrozić życiu lub zdrowiu wielu osób. Rynek energii jest silnie regulowany przez państwo w sposób często skomplikowany i wielopłaszczyznowy. Co więcej, z uwagi na duże znaczenie gospodarcze i polityczne, ilość i różnorodność interesariuszy oraz tradycyjne zaangażowanie państwa w funkcjonowanie rynku, przepisy prawne znajdujące doń zastosowanie są poddawane regularnym i częstym zmianom. Energetyka staje się także coraz częściej celem ataków hakerskich, zarówno ze strony złośliwych jednostek jak i wrogich państw. Rynek wymusza przy tym współpracę podmiotów różniących się względem siebie pod względem charakteru organizacji, celów, potrzeb i możliwości technicznych oraz finansowych, pośrednio łącząc m.in. duże spółki skarbu państwa, prywatnych producentów, dystrybutorów, pośredników, prosumentów. Można spodziewać się, że z biegiem czasu rynek skomplikuje się jeszcze bardziej wraz z kształtowaniem nowych modeli wytwórstwa energetycznego, rozwojem technik magazynowania energii i wprowadzaniem dalszych innowacji (np. inteligentnych liczników). W tej sytuacji, zapewnienie stabilnych dostaw prądu, prawidłowe i szybkie rozliczanie, bilansowanie energii, predykcja awarii i prognozowanie zapotrzebowania i zużycia, stanowiąc będą ogromne wyzwanie dla wszystkich zaangażowanych podmiotów.

Powyższe czyni jednak chmurę szczególnie interesującym rozwiązaniem. Istota usługi tkwi w elastycznym dostosowaniu do potrzeb użytkownika: zarówno pod względem wielkości wymaganych zasobów jak i zakresu wdrożenia. Należy więc ocenić jaki jest bilans korzyści i wad chmury obliczeniowej.

5.2. Ocena przydatności chmury obliczeniowej

Na przykładzie opisanych w rozdziale 4.3 *case studies* widać wyraźnie korzyści związane z korzystaniem z chmury obliczeniowej:

a. skalowalność

- elastyczność dostosowania usług do potrzeb użytkownika: użytkownik może zmniejszać lub zwiększać dostarczaną moc obliczeniową, dodawać nowe stanowiska pracy lub nowych użytkowników, dodawać nowe licencje na oprogramowanie lub rezygnować z posiadanych licencji – wszystko w sposób dynamiczny i samodzielny (bez angażowania dostawcy);
- zminimalizowanie efektu przeskalowania infrastruktury – w razie wystąpienia nadzwyczajnych zdarzeń wymagających od użytkownika dużej mocy obliczeniowej, może on w prosty sposób uruchomić niezbędne zasoby. Nie ma natomiast potrzeby ponoszenia z góry dużych nakładów inwestycyjnych na infrastrukturę fizyczną, która byłaby wykorzystywana na stałe jedynie w niewielkiej części;
- elastyczne narzędzie planowania i użytkowania – użytkownik uzyskuje łatwą możliwość zamówienia zasobów pod konkretny projekt, np. w zakresie R&D i obliczeń macierzowych, bez potrzeby zakupu nowej infrastruktury na konkretny projekt; po sprawdzeniu postawionych tez badawczych, użytkownik może zamknąć projekt bez obaw, że pozostanie ze zbędnym sprzętem;
- praktycznie nieograniczona pojemność przechowywania danych;

b. obniżenie kosztów

- przeniesienie odpowiedzialności za obsługę i infrastrukturę na dostawcę usług chmurowych pozwala znacznie zredukować koszty utrzymania i modernizacji infrastruktury IT;
- wykorzystanie efektu skali uzyskiwanego przez dostawców przekłada się na niższe ceny dla użytkowników;
- uelastycznienie rozliczania wewnątrz organizacji - wydatki inwestycyjne (CAPEX) zamieniane są na bardziej zrównoważone wydatki operacyjne (OPEX);
- elastyczność stosowania – możliwość zakończenia używania niewykorzystywanych funkcjonalności w dowolnym czasie;
- elastyczny model licencyjny;

c. cyberbezpieczeństwo

- dane chronione są wielopoziomowo (przez struktury dostawcy i użytkownika);
- nakłady największych dostawców chmury na cyberbezpieczeństwo (narzędzia, ludzie, zasoby) wykraczają poza możliwości nawet największych polskich przedsiębiorstw energetycznych;
- zapewnienie zgodności z procedurami cyberbezpieczeństwa potwierdzone certyfikatami;
- dostawca aktualizuje licencje i dostarcza najnowsze dostępne rozwiązania (nie dotyczy to modelu IaaS);
- natychmiastowa reakcja na zagrożenia na skalę globalną;

d. szybkość przetwarzania danych

- możliwość monitorowania danych w czasie rzeczywistym;
- skrócenie czasu reakcji na nieplanowane wydarzenia zewnętrzne;

e. innowacyjność i wygoda

- obniżenie kosztów dostępu do najnowszych technologii;
- skrócenie cykli tworzenia nowych rozwiązań systemowych, przyspieszenie rozwoju technologicznego;
- dostęp do danych z każdego miejsca na świecie, z różnych urządzeń;
- łatwa praca zdalna i kolaboracja.

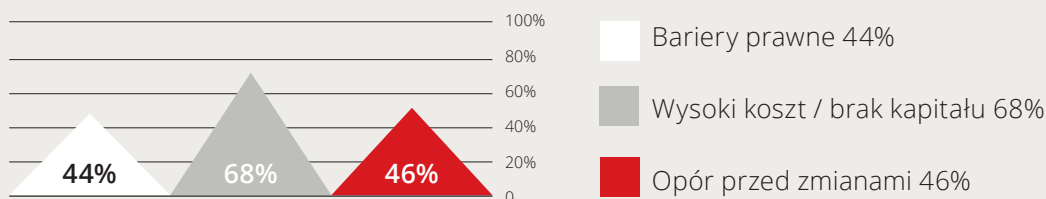
Pomimo przedstawionych wyżej korzyści, wykorzystanie rozwiązań chmury obliczeniowej w polskiej gospodarce pozostaje na stosunkowo niskim poziomie. Jak wyjaśniono na wstępie w 2020 r. jedynie co czwarty przedsiębiorca korzystał z płatnych usług chmury obliczeniowej (24,4%)⁴⁹.

49 GUS: Społeczeństwo informacyjne w Polsce w 2020 roku, 16.12.2020.

Wydaje się, że niskie wykorzystanie chmury w sektorze prywatnym jest związane z niewystarczającym rozpoznanem technologii przez rynek. Okazuje się bowiem, że korzyści chmury identyfikowane powszechnie w popularnych opracowaniach tematu (niskie koszty, bezpieczeństwo danych) są również często wskazywane jako potencjalna bariera dla wdrożenia.

PRZYKŁADOWO, WŚRÓD NAJCZĘSTSZYCH BARIER HAMUJĄCYCH ROZWÓJ CHMURY W SEKTORZE PRYWATNYM WYMIENIA SIĘ:

Wg badania EY Law Compass⁵⁰



Wg badania Computerworld⁵¹:



⁵⁰ Raport EY Law Compass. Prawo i innowacje. Wyzwania 2020.

⁵¹ Badanie przeprowadzone przez portal Computerworld we współpracy z Google oraz ITMagination: <https://www.computerworld.pl/news/Adaptacja-chmury-obliczeniowej-w-Polsce-i-na-swiecie,409498.html>; podobne czynniki identyfikują również inne źródła: zob. np. T. Parys: Cloud Computing – Korzyści i bariery wdrożenia oraz ich przejawy w ocenie użytkowników, marzec 2015, <https://www.researchgate.net/publication/304253902> (badanie empiryczne na próbie 92 osób; zob. także: https://biznes.newseria.pl/biuro-prasowe/it_i_technologie/chmura-mozliwosci-dla,b259896807; CloudPassage Cloud Security Spotlight Report - <https://pages.cloudpassage.com/rs/857-FXQ-213/images/cloud-security-survey-report-2016.pdf>).

Aby ocenić wpływ powyższych czynników na bilans korzyści i wad chmury obliczeniowej, w dalszej części raportu postanowiliśmy odpowiedzieć na 4 kluczowe pytania:

- a. Czy korzystanie z chmury obliczeniowej w energetyce jest zgodne z prawem?
- b. Czy korzystanie z chmury nie zagrazi bezpieczeństwu danych?
- c. Czy korzystanie z chmury „się opłaca”?
- d. Czy moja organizacja słusznie obawia się wdrożenia chmury?

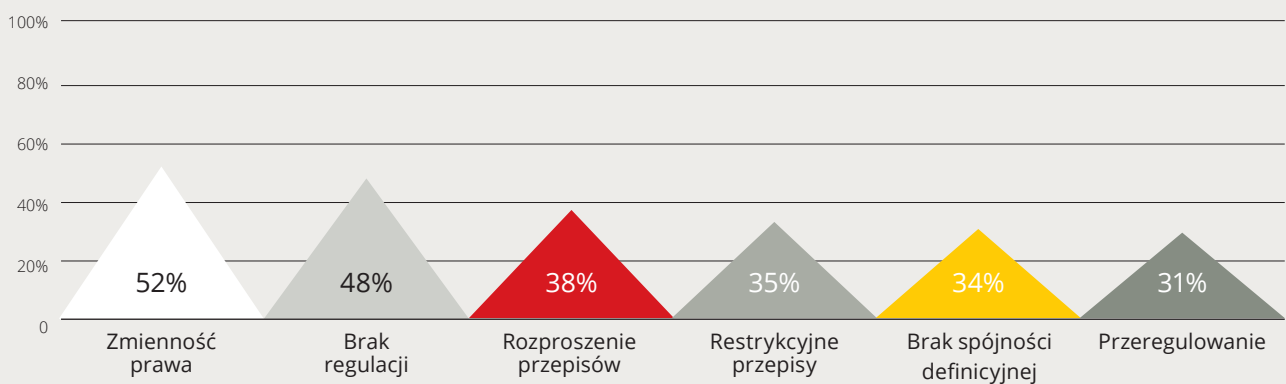
5.2.1. Czy korzystanie z chmury obliczeniowej w energetyce jest zgodne z prawem?

Swoboda działalności gospodarczej

Brak zakazów wykorzystania chmury obliczeniowej

Bariery prawne hamujące wykorzystanie nowych technologii w energetyce związane są z ogólnie pojętą trudnością legislacji. Z jednej strony, ankietowani wymieniają dużą zmienność przepisów, przeregulowanie i restrykcje prawne, jako czynniki utrudniające implementację nowych technologii. Z drugiej, dostrzegają brak uregulowania istotnych obszarów i brak spójności definicji.

CO ANKIETOWANI POSTRZEGAJĄ JAKO BARIERY HAMUJĄCE WYKORZYSTANIE NOWYCH TECHNOLOGII W ENERGETYCE⁵²



52 Opracowano na podstawie danych zawartych w Raporcie EY Law Compass. Prawo i innowacje. Wyzwania 2020.

Wbrew pozorom, wnioski te nie są wzajemnie sprzeczne. Z uwagi na znaczenie dla bezpieczeństwa państwa i potencjał ekonomiczny największych spółek energetycznych kraju, sektor energii jest sektorem silnie uregulowanym na wielu, różnorodnych płaszczyznach. Prawnicy i zarządy firm energetycznych każdego dnia stają przed trudnym wyzwaniem stosowania skomplikowanych, często zmienianych i potencjalnie wzajemnie sprzecznych regulacji prawnych, które utrudniają wdrażanie innowacji i poszukiwanie przewagi konkurencyjnej. To może rodzić pokusę do działania zachowawczego, defensywnego, nastawionego na ograniczanie ryzyk, ze stratą dla istotnych korzyści gospodarczych związanych z chmurą.

Tymczasem, **obowiązujące prawo nie zawiera przepisów zakazujących korzystania z chmury w energetyce**. Jednocześnie obowiązujące przepisy nie regulują precyzyjnie warunków jej wdrożenia i wykorzystywania w działalności. Takie przepisy podwyższałyby pewność prawa i komfort decydentów z sektora energetyki, potencjalnie wpływając na poprawę innowacyjności sektora.

Podkreślić jednak należy, że zgodnie z zasadą „*co nie jest zakazane jest dozwolone*”, brak wyraźnych mechanizmów regulujących implementację chmury nie stanowi przeszkody dla jej wdrożenia w energetyce. Podstawą polskiego ustroju gospodarczego jest wolność gospodarcza, podkreślona w art. 20 Konstytucji Rzeczypospolitej Polskiej⁵³ oraz art. 2 ustawy prawo przedsiębiorców⁵⁴. Zasada ta doznawać może ograniczeń wynikających z przepisów prawa⁵⁵, np. w zakresie wymogu uzyskania koncesji dla niektórych działalności (np. koncesja na poszukiwanie złóż kopaliny), czy stosowania się do pewnych szczególnych warunków obowiązujących na rynkach regulowanych. Obowiązujące przepisy nie zawierają jednak norm zakazujących korzystanie z chmury obliczeniowej w energetyce. W istocie, jak już była mowa polskie i unijne organy publiczne zachęcają do zwiększania wykorzystania rozwiązań chmurowych w sektorze publicznym i prywatnym (rozdział 4.2). Wiele spółek energetycznych w Polsce i Europie już stosuje rozwiązania chmurowe⁵⁶ (rozdział 4.3).

Co istotne, technologia chmur jest wdrażana również w innych, równie mocno regulowanych rynkach co energetyka: np. w finansach i ubezpieczeniach czy branży zdrowotnej. Spółki działające na tych rynkach mają dostęp do danych wyjątkowo wrażliwych, są poddane nadzorowi i rozproszonym regulacjom krajowym oraz europejskim, a dodatkowo nierzadko, muszą sprostać wymogom różnych, potencjalnie sprzecznych jurysdykcji i wewnętrznym zasadom korporacyjnym wiążącym duże grupy kapitałowe.

53 „Społeczna gospodarka rynkowa oparta na **wolności działalności gospodarczej**, własności prywatnej oraz solidarności, dialogu i współpracy partnerów społecznych stanowi podstawę ustroju gospodarczego Rzeczypospolitej Polskiej.” – art. 20 Konstytucji Rzeczypospolitej Polskiej z 2 kwietnia 1997 r. (Dz.U. Nr 78, poz. 483 ze zm.).

54 „Podejmowanie, wykonywanie i zakończenie działalności gospodarczej jest wolne dla każdego na równych prawach” – art. 2 ustawy prawo przedsiębiorców z dnia 6 marca 2018 r. (Dz.U. z 2018 r. poz. 646 z późn. zm.)

55 Zasada ta została podkreślona już w art. 22 Konstytucji Rzeczypospolitej Polskiej: „Ograniczenie wolności działalności gospodarczej jest dopuszczalne tylko w drodze ustawy i tylko ze względu na ważny interes publiczny.”

56 Por. rozdział [...].

Pewne ułatwienie mogą jednak stanowić branżowe opracowania oraz wytyczne regulatora. Nie ma wątpliwości, że wydane przez KNF w 2017 r. i 2020 r. wytyczne na temat stosowania chmur obliczeniowych ułatwią przyjęcie technologii w sektorze, poprzez zwiększenie pewności i jasności prawa. Podobne wytyczne powinny zostać wydane przez rząd i regulatorów rynku energetyki.

Chmura a ochrona danych.

Zasada swobodnego przepływu danych w UE.

Podstawową zasadą prawodawstwa UE zwiększającą pewność prawa użytkowników chmury jest zasada wolnego przepływu danych w granicach UE. Zasada ta obejmuje zarówno dane nieosobowe jak i dane osobowe.

- a. **Dane osobowe** – informacje o (i) zidentyfikowanej lub (ii) możliwej do zidentyfikowania osobie. Danymi osobowymi są więc dane identyfikujące daną osobę (imię, nazwisko, PESEL), ale też jakiegokolwiek informacje o ile dotyczą konkretnej osoby, w tym np. preferencje wyborcze, informacje o zużyciu prądu i stosowanej taryfie, rachunkach za energię elektryczną, czy miejscu zamieszkania⁵⁷. Ich przetwarzanie reguluje Rozporządzenie 2016/679 (tzw. Rozporządzenie RODO)⁵⁸.
- b. **Dane nieosobowe** – dane inne niż dane osobowe, w tym np. zagregowane i zanonimizowane zbiory danych wykorzystywane w procesach big data⁵⁹. Ich przetwarzanie reguluje Rozporządzenie 2018/1807⁶⁰.
- c. **Przetwarzanie** – każda operacja na danych osobowych, w tym zautomatyzowana, np. przetwarzanie, zbieranie, przesyłanie, analizowanie, edycja, usuwanie, ujawnianie, kopiowanie⁶¹.

57 Art. 4 pkt 1 Rozporządzenia 2016/679.

58 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

59 Motyw 9 Rozporządzenia 2018/1807 jako przykład takich danych wymienia dane związane z rolnictwem precyzyjnym ułatwiające monitorowanie i optymalizację zużycia pestycydów i wody lub dane dotyczące potrzeb związanych z konserwacją maszyn przemysłowych.

60 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej.

61 Art. 4 pkt 2 Rozporządzenia 2016/679.

Dane nieosobowe

W zakresie danych nieosobowych prawo UE oparte jest na zasadzie swobodnego przepływu danych. Zasada ta doznaje ograniczeń jedynie ze względu na bezpieczeństwo publiczne, jednak nawet wtedy zastosowanie takiego ograniczenia wymaga otrzymania zgody ze strony Komisji Europejskiej. Jak wskazano w motywie 18 Rozporządzenia 2018/1807:

„Wymogi dotyczące lokalizacji danych stanowią niewątpliwą przeszkodę dla swobody świadczenia usług przetwarzania danych w Unii oraz dla rozwoju rynku wewnętrznego. Powinny one zatem zostać zakazane, chyba że są uzasadnione względami bezpieczeństwa publicznego”

Co ważne, Rozporządzenie 2018/1807 jest neutralne technologicznie. Chroni więc swobodę przesyłania danych nieosobowych niezależnie od stosowanego modelu i jego intensywności, w tym, jak wskazuje jego motyw przewodni nr 17:

- a. przechowywanie danych (infrastruktura jako usługa, ang. Infrastructure-as-a-Service, IaaS);
- b. przetwarzanie danych na platformach (platforma jako usługa, ang. Platform-as-a-Service, PaaS);
- c. przetwarzanie danych w aplikacjach (oprogramowanie jako usługa, ang. Software-as-a-Service, SaaS).

Bezpieczeństwo publiczne na gruncie Rozporządzenia 2018/1807 rozumiane jest szeroko jako bezpieczeństwo wewnętrzne i zewnętrzne, chroniące przed zagrożeniami dla podstawowych interesów społecznych, takich jak zagrożenie „funkcjonowania instytucji i podstawowych usług publicznych oraz życia ludności, a także ryzyko poważnego zakłócenia stosunków zagranicznych lub pokojowego współistnienia narodów lub zagrożenie dla interesów wojskowych.”⁶² Można wyobrazić sobie więc wprowadzenie przez polskiego ustawodawcę ewentualnych ograniczeń w transferze szczególnego rodzaju danych nieosobowych w sektorze energetyki poza Polskę. Takie ograniczenie musiałyby jednak być wąskie, proporcjonalne do chronionego interesu i dotyczyć wyraźnie wskazanych kategorii danych⁶³. Nawet jednak bez takich ograniczeń, kluczowe jest, aby przedsiębiorstwa z sektora energetyki zachowały ostrożność w korzystaniu z chmury obliczeniowej, kierując się bezpieczeństwem danych i sieci. To nie powinno jednak stanowić pretekstu dla niewdrażania innowacji; biznesowo lepszym rozwiązaniem jest korzystanie z dostępnych narzędzi technicznych i prawnych zabezpieczających kontrolę, integralność i dostępność danych.

62 Por. motyw 19 Rozporządzenia 2018/1807.

63 Odrębne ograniczenia mogą wynikać z zasad szczególnych dla pewnych stosunków, np. zasad ochrony informacji niejawnych zgodnie z ustawą o ochronie informacji niejawnych z dnia 5 sierpnia 2010 r. (Dz.U. nr 182, poz. 1228 z późn. zm.)

Dane osobowe

Również regulacje danych osobowych nie stanowią przeszkody dla korzystania z chmury obliczeniowej. **Przed wszystkim, prawo UE nie zakazuje przetwarzania danych osobowych i nie ogranicza swobodnego przepływu danych osobowych w UE.** Celem UE było znalezienie kompromisu pomiędzy zapewnieniem swobodnego przepływu danych osobowych a ich ochroną:

„Technologia zmieniła gospodarkę i życie społeczne i powinna nadal ułatwiać swobodny przepływ danych osobowych w Unii oraz ich przekazywanie do państw trzecich i organizacji międzynarodowych, równocześnie zaś powinna zapewniać wysoki stopień ochrony danych osobowych.”⁶⁴

Kompromis ten realizowany jest poprzez wymogi, jakie muszą być zachowane, aby przetwarzanie danych (w tym przesyłanie z wykorzystaniem chmury) było dopuszczalne. Przed wszystkim dysponent danych osobowych zachowuje nad nimi kontrolę, a jego zgoda stanowi najważniejszą podstawę przetwarzania. Dysponent danych osobowych musi być także odpowiednio informowany o zasadach przetwarzania.

Każdy z tych wymogów może być z powodzeniem realizowany w środowisku chmury obliczeniowej.

Przetwarzanie danych osobowych przez dostawców chmury. Prawo zezwala również na przechowywanie i przesyłanie danych osobowych w środowisku chmury, o ile dostawca chmury zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Powierzenie przez administratora przetwarzania danych osobowych wymaga zawarcia umowy w której należy określić m.in. przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora oraz podmiotu przetwarzającego. W praktyce, wymogi te będą realizowane za pośrednictwem regulaminów dostawców chmury.

Przesyłanie danych poza granice Europejskiego Obszaru Gospodarczego. Kolejnym potencjalnym problemem w zakresie danych osobowych są obostrzenia związane z transferem danych poza Europejski Obszar Gospodarczy.

64 Motyw 6 Rozporządzenia 2016/679.

RODO nie zakazuje tego typu transferów, pod warunkiem spełnienia dodatkowych wymogów, w tym przede wszystkim zapewnienia odpowiedniego poziomu ochrony danych. W praktyce podstawą transferu danych osobowych poza EOG z wykorzystaniem usług chmury są najczęściej tzw. standardowe klauzule umowne. Tego typu klauzule stosują najwięksi dostawcy usług chmury, którzy jednocześnie podejmują szereg działań mających na celu zapewnienie zgodności z prawem UE⁶⁵.

Jak wynika z rekomendacji Europejskiej Rady Ochrony Danych, standardowe klauzule umowne powinny być wspierane środkami uzupełniającymi o charakterze technicznym i kontraktowym, jak szyfrowanie lub anonimizacja danych, gwarantującymi ochronę danych osobowych poza EOG na poziomie odpowiadającym ochronie danych w UE⁶⁶. Tego typu obowiązki nie stoją jednak na przeszkodzie wykorzystania chmury obliczeniowej. Powinny za to być uwzględnione na etapie przygotowania do wdrożenia (por. rozdział 6).

Odpowiedzialność administratora danych. Co do zasady administrator danych osobowych ponosi odpowiedzialność odszkodowawczą związaną z naruszeniem przepisów RODO w pełnym zakresie. Administrator odpowiada m.in. za zapewnienie odpowiedniego bezpieczeństwa danych, uwzględniając aktualny stan wiedzy technicznej (art. 32 RODO). To może wiązać się z koniecznością ponoszenia wysokich nakładów na zabezpieczenie przetwarzanych danych przed dostępem osób trzecich i – w razie naruszenia przepisów – odpowiedzialność odszkodowawczą oraz administracyjną. Przetwarzanie danych z wykorzystaniem chmury w pewnym sensie ułatwia dochowanie powyższym wymogom. Wraz z powierzeniem przetwarzania danych dostawcy chmury, dostawca odpowiada za zapewnienie zgodności z przepisami RODO. W praktyce oznacza to, że to dostawca zapewnia bezpieczeństwo danych przechowywanych w chmurze, wykorzystując ku temu własne zasoby i specjalistyczne systemy (por. rozdział 5.2.2 poniżej).

5.2.2. Czy korzystanie z chmury obliczeniowej nie zagraża bezpieczeństwu danych?

Cyberbezpieczeństwo przedsiębiorstw sektora energetyki jest szczególnie istotne z uwagi na ich znaczenie dla bezpieczeństwa państwa. Ze względu na uzależnienie od energii elektrycznej społeczeństwa, nawet krótkotrwała przerwa w dostawie może spowodować znaczne szkody w przemyśle, systemie opieki zdrowotnej i środowisku. Prawidłowe funkcjonowanie sektora energetyki jest też kluczowe dla właściwego bilansowania krajowego wytwórstwa. Jak wskazano w Krajowym Planie Zarządzania Kryzysowego:

65 Przykładowo, Microsoft ogłosił dodatkowe mechanizmy umowne w ramach programu Defending Your Data (<https://blogs.microsoft.com/on-the-issues/2020/11/19/defending-your-data-edpb-gdpr/>).

66 Oparcie na standardowych klauzulach umownych wymaga m.in. każdorazowej oceny, czy w danym państwie trzecim przestrzegany jest wymagany stopień ochrony danych, a przyjęte środki gwarantują ochronę danych na poziomie wynikającym z prawa UE. Jeżeli tak nie jest, konieczne jest stosowanie środków uzupełniających, w tym technicznych (anonimizacja danych, szyfrowanie) – por. rekomendację Europejskiej Rady Ochrony Danych 01/2020 w sprawie środków uzupełniających przesył danych (https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en); zob. także wytyczne Grupy Roboczej art. 29 ds. Ochrony Danych przedstawione w Opinii 5/2012 z dnia 1 lipca 2012 r. w sprawie przetwarzania danych w chmurze obliczeniowej.

“Charakterystyczne cechy energii elektrycznej takie jak brak możliwości magazynowania ilości mogących zaspokoić nawet krótkotrwałe zapotrzebowanie odbiorców oraz ekstremalnie krótki czas pomiędzy wytworzeniem i zużyciem sprawiają, że system elektroenergetyczny nie dysponuje bezwładnością pozwalającą na jakiegokolwiek przerwy w dostawach bez odczuwalnych konsekwencji dla odbiorców.”⁶⁷

Dlatego też część przedsiębiorców energetycznych objęta jest szczególnymi obowiązkami wynikającymi z ustawy o zarządzaniu kryzysowym⁶⁸ i krajowym systemie cyberbezpieczeństwa⁶⁹. Ustawy te nie zawierają jednak przeciwwskazań dla korzystania z chmury obliczeniowej, a ustawa o krajowym systemie cyberbezpieczeństwa wprost wskazuje możliwość wykorzystania Dostawców Usług Cyfrowych (w tym dostawców chmury obliczeniowej) do realizacji usług kluczowych. Cały sektor energetyki jest jednak jednym z najczęstszych celów ataków hakerskich⁷⁰. Przykładowo:

- a. w latach 2015-2017 r. ataki hakerskie doprowadziły do poważnych zakłóceń prądu na Ukrainie, wywołując m.in. blackout w Kijowie. Ponad 200.000 osób straciło prąd na kilka godzin⁷¹;
- b. w 2017 r. hakerzy próbowali spenetrować systemy amerykańskich operatorów elektrowni atomowych⁷²;
- c. w 2017 r. hakerzy uzyskali dostęp do nieszyfrowanej komunikacji irlandzkiego operatora sieci EirGrid, próbując włamać się do systemu i potencjalnie zakłócić działanie całej sieci⁷³.

Według najnowszych badań, 94% ankietowanych specjalistów bezpieczeństwa uważa, że pandemia zwiększa poziom zagrożenia cybernetycznego, a 25% uznało je za krytyczne⁷⁴. Prognozuje się, że w 2021 r. przedsiębiorca będzie padał ofiarą ataku typu ransomware co **11 sekund**. 34% spółek dotkniętych takim atakiem potrzebuje przynajmniej jednego tygodnia na przywrócenie funkcjonalności⁷⁵. Korzystanie z chmury obliczeniowej może pomóc przedsiębiorcom energetycznym w zarządzaniu ryzykiem cybernetycznym. Według danych za 2020 r. infrastruktura chmury publicznej miała doznać aż 60% mniej incydentów bezpieczeństwa od tradycyjnych centr danych⁷⁶. W efekcie, według jednego z badań 61% ankietowanych ekspertów bezpieczeństwa uważa, że usługi chmury są bardziej bezpieczne niż korzystanie z tradycyjnej infrastruktury⁷⁷.

67 Krajowy Plan Zarządzania Kryzysowego, cz. B, s. 205.

68 Zgodnie z ustawą ustawa o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 r. (Dz.U. Nr 89, poz. 590 z późn. zm.)

69 Zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 r. (Dz.U. z 2018 r. poz. 1560 z późn. zm.)

70 Zob. <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks>; <https://www.hornetsecurity.com/en/security-information/cybersecurity-special-energy-sector/>.

71 Zob. np. <https://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA>.

72 Zob. <https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html>.

73 Zob. <https://www.independent.ie/irish-news/state-sponsored-hackers-targeted-eirgrid-electricity-network-in-devilish-attack-36005921.html>.

74 Deloitte Technology, Media and Telecommunications Predictions 2021, s. 19.

75 Zob. <https://phoenixnap.com/blog/ransomware-statistics-facts>.

76 Gartner, Cloud Strategy Leadership, s. 14.

77 Zob. https://www.ey.com/en_gl/alliances/what-every-cfo-needs-to-know-about-the-cloud?_lsrc=c1f086ee-53bf-409b-a4e9-80795888be57

Powodów dla przewagi bezpieczeństwa rozwiązań chmury jest co najmniej kilka:

- a. **Integralność systemu.** System jest tak bezpieczny jak jego najsłabsze ogniwo. Najwięcej incydentów bezpieczeństwa związana jest z działaniem człowieka. W zintegrowanym systemie chmurowym dużo łatwiej przeszkolić kadry do zachowania kluczowych podstaw bezpieczeństwa i nadzorować w pewnym stopniu przestrzeganie ustanowionych zasad. Rozwiązania chmurowe mają charakter homogeniczny: stanowią nową technologię, budowaną od podstaw z założeniem najwyższych standardów bezpieczeństwa. W przeciwieństwie do chmury obliczeniowej, infrastruktura IT spółek energetycznych składa się często z szeregu połączonych ze sobą systemów i aplikacji, dodawanych stopniowo na przestrzeni wielu lat przez potencjalnie różnych wykonawców, stosujących różne standardy bezpieczeństwa. W rezultacie mogą być dotknięte większą ilością podatności na zagrożenie.
- b. **Rozwój, aktualizacje.** Bezpieczeństwo sieci stanowi kluczowy aspekt budujący reputację czołowych dostawców usług chmury obliczeniowej. Dlatego też wykorzystują oni najnowocześniejszą infrastrukturę, odpowiadają za aktualizację, spełnianie norm ISO i procesy certyfikacyjne, nadzorują dostawców i pracowników, a także podejmują działania operacyjne, administracyjne, prawne, przygotowawcze i techniczne mające na celu utrzymywanie najwyższych zabezpieczeń systemów, np. stałe audyty i testy. Zdecydowana większość zespołów IT spółek energetycznych nie jest w stanie z tym konkurować, m.in. z uwagi na ograniczone zasoby (finansowe, ludzkie, sprzętowe) oraz nieporównywalnie mniejszą zatrudnienia czołowych światowych specjalistów z zakresu bezpieczeństwa.
- c. **Redundancja.** Korzystanie z chmury pozwala na przechowywanie i przetwarzanie danych z wykorzystaniem centrów danych w różnych miejscach geograficznych, eliminując tym samym zagrożenia związane z fizycznym uszkodzeniem lub nieodostępnością danych (brak zasilania) czy ataki nakierowane na jedną serwerownię, w której przechowywane są dane.

Podkreślić należy, że korzystanie z usług chmury samo w sobie nie zastąpi wewnętrznych procedur cyberbezpieczeństwa, choć wymusza ich ustandaryzowanie i ujednoczenie, dzięki czemu przeszkolenie kadr i egzekucja zasad jest prostsza. Usługi w chmurze również zdarzają się być przedmiotem ataków hakerskich, tyle, że zwykle wynikają one z błędów ludzkich leżących po stronie organizacji, a nie dostawcy chmury, np. braku obowiązkowego szyfrowania połączeń, korzystania z VPN, dwustopniowej autoryzacji przy próbach logowania do serwerów służbowych z prywatnych urządzeń, nieostrożności użytkownika klikającego w nieznane linki (ataki typu *phishing*) czy wykorzystywanie tego samego hasła na potrzeby różnych portali i stron⁷⁸. Często hakerzy uzyskują dostęp do danych przechowywanych w chmurze pośrednio, po przełamaniu zabezpieczeń fizycznej infrastruktury organizacji (komputera użytkownika czy serwerów fizycznych)⁷⁹. Tego typu zaniedbania po stronie organizacji otwierają pole do ataków nawet najlepiej zabezpieczonych usług w chmurze.

78 Zob. <https://threatpost.com/cloud-attacks-bypass-mfa-feds/163056/>.

79 Zob. National Security Agency (NSA), Detecting Abuse of Authentication Mechanisms, https://media.defense.gov/2020/Dec/17/2002554125/-1/-1/0/AUTHENTICATION_MECHANISMS_CSA_U_OO_198854_20.PDF.

Bezpieczeństwo danych i organizacji to jednak coś więcej niż tylko ochrona przed hakerami. Z perspektywy energetyki bardzo istotne jest zapewnienie, aby korzystanie z chmury nie powodowało jakichkolwiek przesto-
 jów w pracy, np. z uwagi na zmiany regulacyjne dotyczące dostawcy, problemy sieciowe w państwie, gdzie
 zlokalizowane są centra danych czy problemy techniczne po stronie dostawcy. Przedsiębiorcy muszą także
 zapewnić sobie elastyczność dalszych zmian, w tym nawet zmiany dostawcy usług chmury. Tego typu potrzeby
 powinny jednak być adresowane na etapie wdrożenia, poprzez stosowne mechanizmy techniczne, organiza-
 cyjne i kontraktowe (zob. rozdział 6). Technologia chmury jako taka w żaden sposób nie stoi na przeszkodzie
 realizacji tych celów.

Można spodziewać się, że w najbliższych latach organy państwowe wydadzą wytyczne uszczegóławiające tech-
 niczne wymogi wykorzystania chmury w sektorach kluczowych dla bezpieczeństwa państwa. Takie działania
 już są prowadzone. Ministerstwo Cyfryzacji opracowało tego typu wymogi dla projektów prowadzonych przez
 podmioty sektora finansów publicznych⁸⁰, zwiększając tym samym pewność prawa kluczowych interesariu-
 szy administracji. Z kolei Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) pracuje nad systemem
 wspólnotowej certyfikacji usług chmurowych⁸¹ a Komisja Europejska wydała zalecenia 2019/553 z 3 kwiet-
 nia 2019 r. w sprawie cyberbezpieczeństwa w sektorze energetycznym. Rekomendowane jest, aby podobne
 wytyczne dla sektora energetyki zostały wydane przez polski rząd we współpracy z ministerstwem cyfryza-
 cji, tak aby ułatwić adopcję rozwiązań chmury obliczeniowej i przyspieszyć rozwój polskich przedsiębiorstw
 energetycznych, jednocześnie zapewniając bezpieczeństwo dostaw energii.

5.2.3. Czy korzystanie z chmury obliczeniowej „się opłaca”?

Kolejnym czynnikiem hamującym implementację chmury w biznesie jest obawa o wysokie koszty wdrożenia
 i korzystania z chmury. Obawy te kontrastują z popularnymi opracowaniami i przekazami marketingowymi,
 w których oszczędności związane z wdrożeniem chmury podaje się jako jedną z głównych korzyści tej tech-
 nologii⁸².

Zbudowanie ogólnego modelu pozwalającego na szacowanie średnich kosztów wdrożenia i korzystania z chmury
 dla przeciętnego przedsiębiorstwa jest niemożliwe. Koszty infrastruktury IT różnią się w zależności od sek-
 tora, potrzeb przedsiębiorstwa i zespołu IT. Brak jest przy tym publicznie dostępnych danych statystycznych
 pokazujących tego typu koszty na odpowiednio dużej grupie podmiotów. Dodatkowo, wiele dużych przedsię-
 wiorstw rozlicza się z dostawcami chmury na podstawie uzgodnionych indywidualnie i poufnych warunków.

Możliwe jest natomiast zidentyfikowanie pewnych zależności, pozwalających na wstępne oszacowanie kosz-
 tów wdrożenia technologii chmury. Szacunki te powinny zostać uzupełnione o indywidualne analizy kosz-
 towe poprzedzające konkretne wdrożenie i uwzględniające specyfikę danego przedsiębiorstwa. Co ważne,

80 Ministerstwo Cyfryzacji, Narodowe Standardy Cyberbezpieczeństwa – Standardy Cyberbezpieczeństwa Chmur Obliczeniowych, luty 2020 r.

81 <https://ec.europa.eu/digital-single-market/en/news/towards-more-secure-and-trusted-cloud-europe>

82 Zob. np. Raport „Chmura nad Polską”, Impact, Fintech, 2019 r., s. 12.

ewentualna analiza powinna koncentrować się na szacowaniu kosztów wdrożenia chmury jako odpowiedzi na konkretny problem organizacyjny, a nie jako ogólną zmianę używanych systemów. Przykładowo, o ile wyliczenie kosztów przejścia całej organizacji do chmury byłoby bardzo trudne i wymagało poczynienia wielu założeń, o tyle szacowanie kosztów realizacji w chmurze konkretnego projektu wymagającego analizy wielkich zbiorów danych, zakupu serwerów, licencji i wyszkolenia personelu może dawać bardziej realne i wiarygodne wyniki.

Konserwatywny model szacowania kosztów chmury opiera się na porównaniu kosztów zakupu i utrzymania fizycznej infrastruktury IT z kosztami chmury (model TCO). Koszt fizycznej infrastruktury IT cechuje duży początkowy nakład inwestycyjny i regularne nakłady utrzymaniowe. Istotą chmury jest dostosowanie kosztu do rzeczywistego zużycia, pod warunkiem jej prawidłowej optymalizacji. Realne koszty mogą różnić się w zależności od sposobu wykorzystania chmury, doświadczenia zespołu IT przedsiębiorcy czy warunków uzgodnionych z dostawcą (np. w zależności od oczekiwanego poziomu SLA).

Oszczędności w stosunku do utrzymania fizycznej infrastruktury IT związane są przede wszystkim ze zmianą charakteru kosztów, z dużych nakładów inwestycyjnych na elastyczne nakłady operacyjne dostosowane do rzeczywistego zapotrzebowania. Zastąpienie fizycznej infrastruktury IT rozwiązaniami chmury pozwala na uniknięcie:

- a. nakładów inwestycyjnych na zakup infrastruktury IT (infrastruktury sieciowej),
- b. nakładów na utrzymanie, konserwację, naprawy (zużyte okablowanie, części zamienne) niewykorzystywanej dotychczas infrastruktury,
- c. kosztów najmu (kupna) pomieszczeń serwerowni,
- d. kosztów prądu i wentylacji serwerowni (w tym kosztów redundantnego zasilania w razie potrzeby zachowania awaryjnych źródeł prądu),
- e. kosztów licencji oprogramowania,
- f. kosztów redundantnych połączeń sieciowych (np. światłowód i awaryjne połączenie satelitarne dla krytycznych usług),
- g. kosztów zabezpieczenia fizycznego (ochrona, kamery).

Główna oszczędność związana jest przede wszystkim z ograniczeniem przestoju w wykorzystaniu infrastruktury i płaceniem tylko za rzeczywiste zużycie (usługa „na żądanie”). Korzyści finansowe dotyczyć więc będą przede wszystkim tych systemów, które cechuje zmienność użycia i które nie wymagają takiej samej mocy obliczeniowej przez 24/7.

Potrzeby IT sektora energetyki cechują się właśnie taką naturą. Spółki energetyczne muszą zapewnić odporność na nadzwyczajne zdarzenia generujące „skoki” wykorzystania infrastruktury (np. wichura zrywająca linie napięcia w regionie, dystrybutorzy otrzymują nawet kilkaset tysięcy zgłoszeń braku prądu w ciągu kilku godzin). Infrastruktura ta budowana była zwykle, przez wiele lat i składa się z szeregu współpracujących ze sobą systemów, wykonanych przez różnych wykonawców. Dlatego:

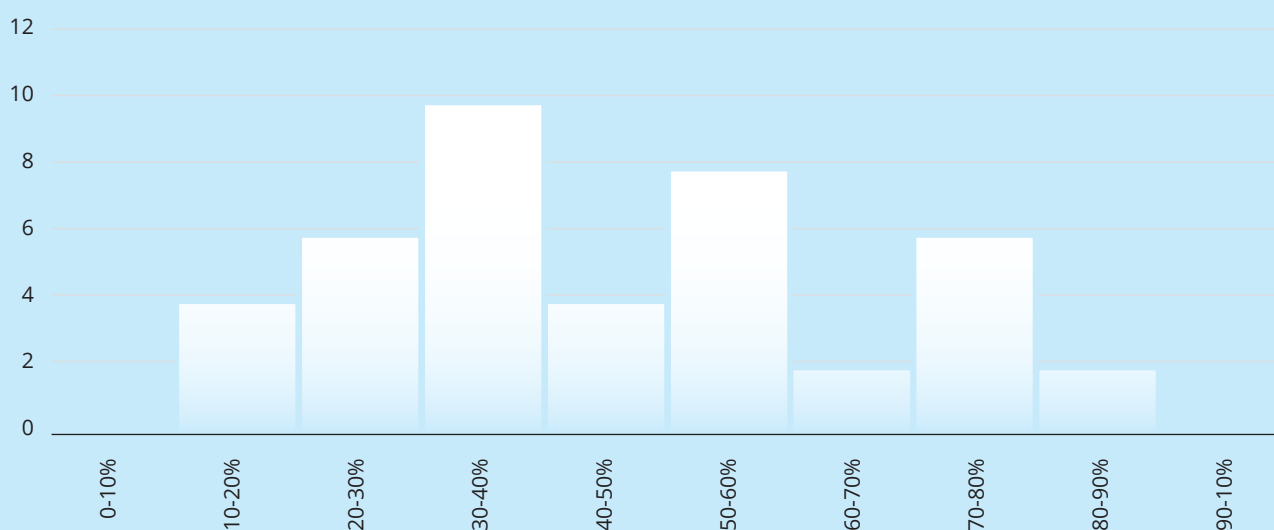
- a. Infrastruktura IT w sektorze energetyki będzie często przeskalowana, aby zapewnić niezbędną redundancję i przygotowanie do obsługi scenariuszy krytycznych. Podobne cechy wykazuje infrastruktura w bankowości, gdzie raportuje się nawet zużycie oscylujące w granicach 30-40% zainstalowanej mocy obliczeniowej⁸³.
- b. Polskie przedsiębiorstwa energetyczne zatrudniają nawet kilkuset osobowe zespoły IT dbające o funkcjonalność wewnętrznych systemów.
- c. Sektor energetyczny musi spełniać najwyższe normy techniczne i standardy bezpieczeństwa. Wydatki na infrastrukturę IT są pomijalne przy stratach wynikających np. z przestoju firmy z uwagi na incydent bezpieczeństwa.
- d. Wykorzystywana infrastruktura jest jednak prostsza niż w wielu spółkach IT i telekomunikacyjnych, istnieje mniej zależności pomiędzy poszczególnymi programami czy systemami, w związku z czym łatwiej jest „rozdzielić” infrastrukturę poszczególnych działów na potrzeby wdrożenia.

Powyższa zależność jest skorelowana z kosztami infrastruktury IT: im większa potrzeba zachowania odporności systemu IT na wypadek sytuacji kryzysowych (skutkującą przeskalowaniem infrastruktury) tym większe będą koszty infrastruktury fizycznej i potencjalnie większa oszczędność związana z wykorzystaniem chmury obliczeniowej z uwagi na elastyczną skalowalność.

Według szacunków International Data Corporation, koszty wdrożenia chmury przynoszą oszczędności, w zależności od modelu wdrożenia, nawet do 60% na zastąpionych kosztach IT: licencjach na oprogramowanie, kosztach sprzętu i powiązanych usług IT⁸⁴. Analiza ponad 20 przypadków wdrożeń wskazuje na to, że średnia oszczędność na kosztach infrastruktury wynosi 48%, przy medianie 45%, a standardowe odchylenie wynosi 20% (co daje oczekiwane wartości oszczędności od 28% do 68%).

83 Zob. PKO Bank Polski, prezentacja „PKO Bank Polski w czasie pandemii”, s. 7: https://www.pkobp.pl/media_files/0400d803-b511-422d-91ba-39411ae2721d.pdf?fbclid=IwAR0S_-IC2KySbNK-dj8dymKAqxMgFmG-Ljp6fsW7azNfEs9CELeByLWtuk.

84 Opracowanie własne na podstawie danych z raportu IDC EMEA na zlecenie Komisji Europejskiej: Uptake of Cloud in Europe, 2014, s. 34. Największe oszczędności odnotowano w modelu SaaS, gdzie 1 euro chmury zastępuje 2.3 euro wydane na tradycyjną infrastrukturę IT; koszt 1 euro w modelu PaaS i IaaS zastępuje 1.8 euro wydatków na tradycyjną infrastrukturę IT.

ODSETEK OSZCZĘDNOŚCI TCO - WDROŻENIE CHMURY⁸⁵

W naszych badaniach nie zidentyfikowaliśmy przypadku dużej spółki, która zanotowała by straty związane z wdrożeniem chmury, co nie oznacza, że takie przypadki nie istnieją. Doniesienia o wysokich kosztach korzystania z chmury pojawiają się w sieci, choć mają często charakter anegdotyczny i anonimowy. Faktem jest jednak, że w bardziej rozwiniętych technologicznie rynkach świata kształtuje się nowy sektor: firm specjalizujących się w optymalizacji kosztów chmury, co może sugerować, że dla niektórych przedsiębiorstw prawidłowe korzystanie z chmury jest wyzwaniem. Nie oznacza to jednak, że chmura jest automatycznie droższa od fizycznej infrastruktury: przeciwnie, **prawidłowo zoptymalizowana chmura odpowiadająca na konkretny problem organizacyjny powinna być w większości przypadków tańszym rozwiązaniem**. Problem pojawia się wtedy, gdy chmura nie jest właściwie wykorzystywana, a wdrożenie nie zostało odpowiednio przygotowane⁸⁶.

Analiza kosztów wdrożenia chmury powinny jednak uwzględniać liczne niewymierne korzyści (rozdział 5.2.4), a także niemożliwe do ogólnego oszacowania oszczędności związane z pracami nad innowacjami i rozwojem biznesu. Przedstawiona wyżej analiza dotyczy problemu migracji dotychczasowych procesów IT do środowiska chmurowego. Naturalne jest jednak, że polski sektor energetyki będzie się rozwijał i poszukiwał nowych rozwiązań technologicznych wspierających działalność operacyjną, m.in. poprzez tworzenie nowych działów,

85 Opracowanie własne na podstawie danych dostępnych publicznie (doniesienia medialne i raporty organizacji zgłaszających oszczędności związane z wdrożeniem chmury). Dane uwzględniają także case studies opisywane przez czołowych dostawców rozwiązań chmury.

86 Zob. np. <https://www.openio.io/blog/are-your-cloud-bills-higher-than-expected-thats-probably-your-fault>

uruchamianie projektów badawczych etc. Tu chmura może okazać się idealnym rozwiązaniem, pozwalającym na ograniczenie kosztów i jednocześnie uzyskanie dostatecznych mocy obliczeniowych do przeprowadzenia niezbędnych analiz w krótkim czasie. Skalowalność chmury pozwala na zaplanowanie i realizację projektów „zasobożernych” bez potrzeby inwestowania w drogą infrastrukturę IT przed weryfikacją postawionych tez badawczych. Chmura może więc pomóc spółkom energetycznym w procesach R&D i działaniach strategicznych, takich jak analizy *big data*, obliczenia macierzowe i AI w procesach predykcji awarii, prognozowania zużycia, zapotrzebowania czy cen surowców. Chmura pozwala więc na uzyskanie korzyści ekonomicznych związanych z brakiem potrzeby inwestowania we własną infrastrukturę dedykowaną dla danego projektu, uzyskaniem szybkich mocy obliczeniowych „na żądanie”, analizą danych w czasie rzeczywistym bez poważniejszych ograniczeń i związanych z tym zwiększeniem efektywności procesów i innowacji.

5.2.4. Czy moja organizacja niesłusznie obawia się wdrożenia chmury?

Ostatnią barierą dla wdrożenia chmury w organizacji są ogólnie rozumiane kwestie organizacyjne: strach przed zmianami, obawa, że nowe rozwiązania wywołają redukcję miejsc prac (dział IT) lub utrudnią pracę, a pracownicy przyzwyczajeni do starych systemów nie będą w stanie znaleźć potrzebnych im danych i dokumentów. Przyjęcie zasady „nie zmieniaj tego, co działa” może pozbawić polskie przedsiębiorstwa istotnych korzyści związanych z wdrożeniem chmury.

Z przeprowadzonych analiz wynika zaś, że zalety chmury z nawiązką rekompensują obawy wewnątrzorganizacyjne związane ze zmianą technologiczną. Omówione na wstępie przykłady wdrożeń (por. rozdział 4.3) uwydatniają takie korzyści jak m.in. łatwość pracy zdalnej i kolaboracji na wspólnych plikach, wideokonferencje, multiplatformowość (dostęp do danych z pozycji mobilnej), szybkość działania programów czołowych dostawców, przyjazne i proste interfejsy, większa pojemność skrzynek emailowych i pełna integracja wszystkich wykorzystywanych narzędzi.

W efekcie, aż 77% badanych przedsiębiorców deklaruje, że posiadane funkcjonalności chmury przekroczyły ich oczekiwania, a 10% uznaje, że przekroczyły je znacznie. Rozczarowanie chmurą deklaruje jedynie 2% użytkowników⁸⁷. Co więcej, większość podmiotów, które wdrożyły chmury w jakimś stopniu planuje pogłębienie wdrożenia. Użytkownicy szczególnie doceniają dostęp do danych w czasie rzeczywistym (59%) oraz skalowalność i dostęp do mocy obliczeniowej (51%) niemożliwej do osiągnięcia w stacjonarnej infrastrukturze⁸⁸.

Powyższe wskazuje, że jeśli **w przypadku chmury „strach ma wielkie oczy”**. Bilans korzyści i wad przemawia za wdrożeniem rozwiązań chmury obliczeniowej w sektorze energetyki, a najpowszechniej identyfikowane bariery nie powinny hamować innowacji polskiego sektora energetyki.

87 Chmura publiczna w Polsce, Deloitte, 2020.

88 Chmura publiczna w Polsce, Deloitte, 2020.



Chmura obliczeniowa nie jest jednak wolna od wyzwań, a wdrożenie musi być odpowiednio przygotowane, żeby w pełni wykorzystać potencjał tej technologii. Omawiane abstrakcyjnie korzyści i wady technologii muszą zostać zweryfikowane w kontekście szczegółowych uwarunkowań wpływających na działania danej organizacji w zakresie technicznym, organizacyjnym, ekonomicznym i prawnym. W przeciwnym wypadku potencjał chmury może zostać niewykorzystany lub wykorzystany nie w pełni, narażając organizację na niepotrzebne koszty.

Podstawowymi błędami wdrożenia są:

- a. niedostosowanie wdrożenia do modelu działalności i potrzeb – chmura jest droższa w działach o stabilnym i stałym zapotrzebowaniu na zasoby obliczeniowe niż w działach, gdzie możemy wykorzystać dynamiczną skalowalność chmury dla dostosowania do rzeczywistych potrzeb;
- b. przeskalowanie chmury - np. przeszacowanie potrzebnej przestrzeni dyskowej, „wykup” większej mocy obliczeniowej niż potrzebne;
- c. brak identyfikacji konkretnych problemów organizacyjnych i projektów, dla których chmura – ze względu na swoją specyfikę – może być rozwiązaniem tańszym i efektywniejszym;
- d. niewystarczające kompetencje działu IT do obsługi i optymalizacji chmury;
- e. niewystarczające kompetencje prawne i organizacyjne;
- f. zbyt optymistyczne estymacje czasu wdrożenia;
- g. niewłaściwy plan wdrożenia z perspektywy przenoszonych działów (np. przeniesienie działu bez przeniesienia systemu plików lub emaili).

Z przeprowadzonych analiz wynika, że większość dużych spółek decydujących się na wdrożenie chmury robi to etapowo, w sposób gwarantujący stabilność działalności operacyjnej. Podkreślić należy więc, że wdrożenie chmury nie musi obejmować całej infrastruktury IT i może zostać ograniczone według potrzeb przedsiębiorcy do:

- a. typowych procesów administracyjnych i biurowych;
- b. danych „niewrażliwych” – np. danych nieosobowych i danych niemających wpływu na bezpieczeństwo infrastruktury krytycznej, danych zanonimizowanych lub zagregowanych;

- c. działów, których zapotrzebowanie jest przystosowane do chmury – działów o mocno zmiennym zapotrzebowaniu na moc obliczeniową (hosting strony internetowej, obsługa klienta);
- d. działów R&D i innowacji, dla których niezbędny jest krótkotrwały dostęp do dużych mocy obliczeniowych;
- e. nowo powstających działów, których dane nie są jeszcze przechowywane w infrastrukturze fizycznej, a wewnętrzne procesy mogą być od początku projektowane z myślą o wykorzystaniu chmury;
- f. czujników zbierających duże ilości danych w czasie rzeczywistym, pozwalających na predykcję awarii czy ocenę zużycia – które mogą być automatycznie przetwarzane w chmurze i udostępniane uprawnionym użytkownikom (pracowników spółki, klientom końcowym, regulatorowi).

Ponadto, z uwagi na odnotowywany opór organizacyjny, wdrożenie chmury warto rozważyć od najprostszych elementów: oprogramowania biurowego, poczty elektronicznej, systemów wideokonferencji. Z prowadzonych rozmów wynika, że rozpoczęcie wdrożenia od tego typu systemów pozwala na oswojenie organizacji ze zmianami i zyskanie przychylności działów IT, otwierając drogę do bardziej innowacyjnych rozwiązań w przyszłości. Tego typu systemy są zaś wystarczające, aby zapewnić organizacji niezbędną elastyczność w niestabilnym czasie pandemii i stale rosnącego trendu pracy zdalnej w sektorze prywatnym.

Bardzo ważne jest, aby przygotowanie wdrożenia obejmowało analizę techniczną, organizacyjną, ekonomiczną i prawną przez heterogeniczny zespół obejmujący przedstawicieli działów zaangażowanych w szeroko rozumiany proces wdrożenia (kadry zarządzające, dział prawny, bezpieczeństwa, compliance, finansowy, IT i danych osobowych). W ten sposób, spółka powinna być w stanie oszacować (i) opłacalność wdrożenia, (ii) zakres wdrożenia, (iii) wymagania techniczne i prawne, które muszą być spełnione. W uproszczeniu, przygotowanie powinno objąć następujące działania:

MATRYCA DZIAŁŃ PRZYGOTOWAWCZYCH

Działania biznesowe i organizacyjne

- ocena potrzeb organizacji i możliwych korzyści wiązanych z wdrożeniem chmury w konkretnych scenariuszach biznesowych
- ocena struktury kadrowej działu IT oraz indywidualnych kompetencji – w zakresie przyszłej obsługi architektury chmury oraz zadań pomocniczych
- wyodrębnienie grup pracowniczych desygnowanych do prowadzenia wdrożenia – ważne, żeby grupa obejmowała pracowników różnych działów (biznes, działy prawne i *compliance*, bezpieczeństwo, dział IT, finanse), aby zapewnić sprawny obieg informacji i niezbędną koordynację
- opracowanie planu przejściowego dla migracji, zidentyfikowanie działów najbardziej wrażliwych na zmiany technologiczne z uwagi na prowadzone czynności
- opracowanie planów szkoleniowych w zakresie podniesienia kompetencji pracowników i kadry zarządzającej

Określenie pryncypiów organizacji w zakresie migracji danych, w szczególności:

- wskazanie zakładanej wydajności migracji (maksymalnego czasu)
- analiza możliwości zatrzymania systemów organizacji i wprowadzenia przestojów
- określenie wielkości (ciężaru) zbiorów danych
- wyodrębnienia danych kluczowych i nadania im priorytetów



Działania prawne

- weryfikacja wdrożenia pod kątem wymogów prawa
- weryfikacja obowiązujących procedur i standardów przetwarzania danych, ocena możliwości klasyfikacji danych (dane osobowe, inne dane chronione prawnie, dane nieosobowe)
- określenie stosowanych zabezpieczeń i podejścia organizacji do przechowywania informacji (istniejącej architektury)
- wyselekcjonowanie grup danych strategicznych dla organizacji
- ocena zadań z zakresu infrastruktury krytycznej (działanie multidyscyplinarne – połączenie działań prawnych, technicznych, organizacyjnych)

Działania finansowe

- Szacowanie opłacalności wdrożenia z uwzględnieniem nakładów na istniejącą lub nową infrastrukturę fizyczną IT (wraz z kosztami ewentualnego utrzymania)
- Porównanie z kosztami chmury o niezbędnej mocy obliczeniowej w zakresie planowanego wdrożenia z uwzględnieniem kosztów utrzymania podwójnej infrastruktury przez okres wdrożenia



Działania techniczne

- weryfikacja infrastruktury IT (*hardware* i *software*) i występujących zależności – m.in. stan techniczny, wiek, stopień zużycia i amortyzacji, okres licencji
- weryfikacja aktualnej wydajności systemów oraz rzeczywistej eksploatacji (kalkulacja efektywności wykorzystania)
- określenie struktur IT krytycznych dla organizacji
- określenie procesów umożliwiających zachowanie ciągłości biznesowej
- określenie ilości i sposobu przechowywania kopii zapasowych
- estymacja prognozowanego zużycia i zapotrzebowania na usługi chmurowe
- określenie maksymalnego zapotrzebowania mocy obliczeniowej (zapotrzebowania szczytowego)
- określenie rodzaju potrzebnego wdrożenia (zakres, model chmury)

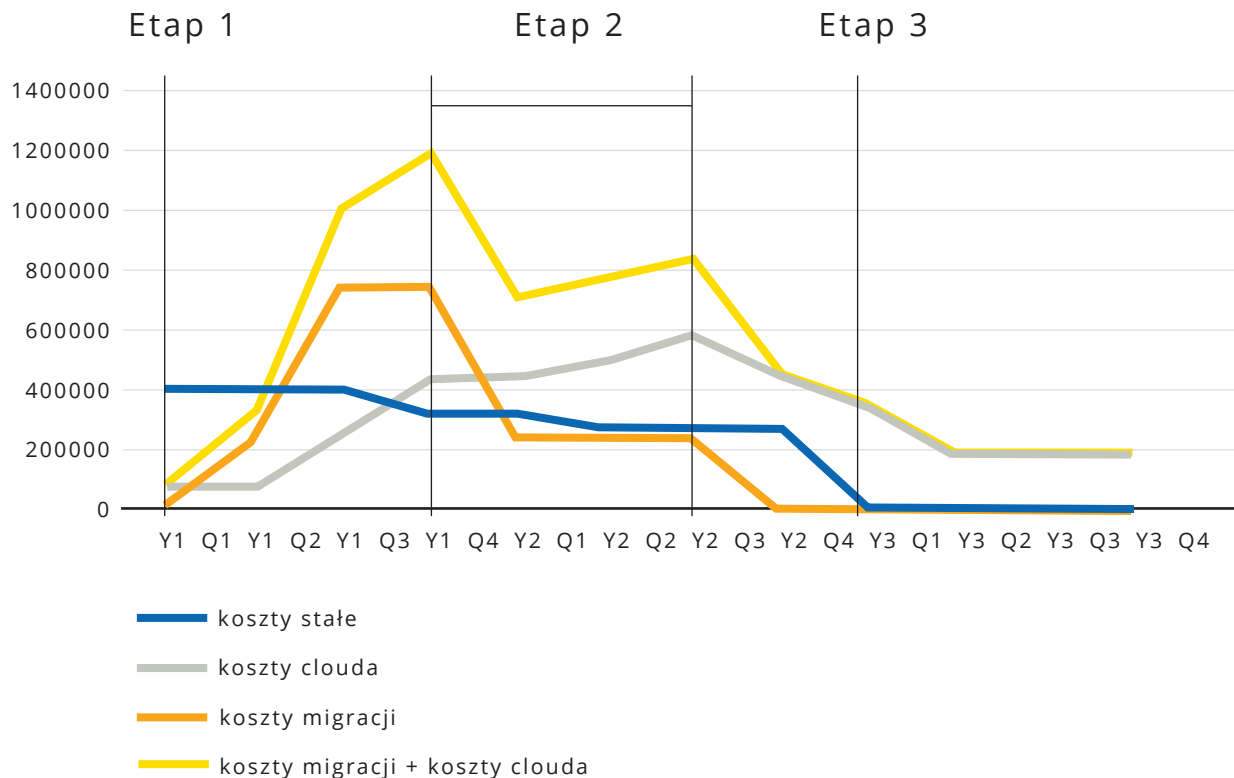


Dopiero szczegółowa, wielopłaszczyznowa analiza pozwoli na prawidłowe przygotowanie wdrożenia i odpowiedzi na kluczowe pytania:

- jaki rodzaj chmury spełni wszelkie oczekiwania organizacji (publiczna, prywatna, hybrydowa, a może *multicloud*)?
- w jakim modelu dostawca będzie świadczył usługi (SaaS, PaaS, IaaS)?
- jaka metoda przenoszenia danych zostanie wykorzystana (jakie narzędzia i o jakiej wydajności będą zastosowane)?
- w jakim zakresie dokonać wdrożenia, które części działalności najlepiej sprawdzą się w chmurze?
- ile czasu zajmie proces wdrożenia?

Szczególną wagę dla osób odpowiedzialnych za wdrożenie powinna mieć odpowiedź na ostatnie z pytań. Im dłuższe wdrożenie tym dłuższy okres, w którym organizacja ponosi podwójne koszty: dotychczasowej infrastruktury fizycznej i chmury. Te podwójne koszty mogą w skrajnych przypadkach być na tyle duże, że w efekcie opóźnią zwrot z inwestycji nawet do 6 lat.

WDROŻENIA NA PODANYCH WYŻEJ PRZYKŁADACH:



Wdrożenie na podanym wyżej przykładzie można podzielić na 3 etapy:

Etap 1 – Testy

Firma zaczyna testować nowe rozwiązania w chmurze, jednocześnie cała dotychczasowa praca wykonywana jest na rozwiązaniach tradycyjnych (na posiadanym sprzęcie). Jest to moment, w którym firma zaczyna ponosić koszty chmury. Część pracowników uczy się i eksperymentuje z chmurą. Następują intensywne szkolenia pracowników, które powodują obniżenie produktywności (spowolnienie innych prac). Firma najczęściej z pomocą zewnętrznego podmiotu dokonuje migracji zasobów i usług do środowiska chmury.

Na tym etapie następuje minimalna lub zerowa redukcja kosztów utrzymania starej infrastruktury.

Etap 2 – Płynne używanie chmury

Pracownicy zaczynają płynnie korzystać z chmury, a większość usług została już przeniesiona lub zduplikowana w chmurze. Firma dostrzega zauważalną, lecz wciąż niewielką obniżkę w kosztach dotychczasowej infrastruktury. Ze względu na coraz większe zaangażowanie wszystkich pracowników w pracę w chmurze następuje niewielki wzrost jej kosztów. Etap ten kończy się w momencie osiągnięcia szczytowej wartości kosztów chmury.

Etap 3 – Wygaszenie starych systemów

Rozwiązania w chmurze są już dobrze znane i istnieje do nich powszechne zaufanie wewnątrz organizacji, co pozwala na wygaszenie starej infrastruktury. Pracownicy uczą się optymalnego wykorzystania zasobów chmury, co przyczynia się do obniżenia jej kosztów. Następuje koniec wydatków związanych z migracją. Etap ten kończy się z całkowitym wygaszeniem starej infrastruktury.

Na podanym wyżej przykładzie, relatywnie długi okres zwrotu związany był z długim okresem wdrożenia, trwającym około 3 lata. Przez ten czas spółka ponosiła podwójny koszt: utrzymania i obsługi fizycznej infrastruktury IT oraz koszty chmury. Dla analizowanego przypadku każdy z poszczególnych etapów trwał około 1 roku. W ciągu 3 lat koszty infrastruktury zostały zredukowane z poziomu 400.000 USD do 190.000 USD, a więc o ponad 50%. **Należy jednak pamiętać, że w okresie tych 3 lat firma poniosła koszty wdrożenia oraz równoległego utrzymywania dwóch infrastruktur.** Okres ten w wielu przypadkach będzie jednak znacznie krótszy, w zależności od intensywności i zakresu wdrożenia (wdrożenie podstawowego poziomu chmury: e-maili i serwerów do przechowywania i wymiany plików powinno być znacznie szybsze), elastyczności organizacji i sprawności zarządu, a także okresów wygaśnięcia poszczególnych umów (np. najmu pomieszczeń, leasingu serwerów, współpracy z podwykonawcą serwisującym serwery, żywotnością posiadanego sprzętu). To potwierdza tylko jak ważne jest odpowiednie przygotowanie wdrożenia.

6.

PODSUMOWANIE I REKOMENDACJE



Usługi chmury obliczeniowej stanowią jedno z najszybciej rozwijających się usług IT na świecie. W niektórych sektorach poziom adopcji chmury jest bardzo wysoki: aż 70% przedsiębiorstw IT i komunikacji w Europie korzysta z płatnych usług chmury. Chmurę wdrażają też podmioty działające na rynkach mocno regulowanych, np. w bankowości czy farmacji. Pomimo tego, korzystanie z chmury wciąż pozostaje niskie w energetyce i sektorze utilities: w 2020 r. jedynie co 3 przedsiębiorca korzystał z tego typu usług.

Pandemia koronawirusa niewątpliwie pokazała jednak, jak ważne usługi chmury mogą okazać się w najbliższej przyszłości. Przedsiębiorstwa korzystające z chmury bez problemu poradziły sobie z wyzwaniami pracy zdalnej. Ich pracownicy otrzymali proste w obsłudze i przyjazne dla użytkowników narzędzia do wymiany plików, wideokonferencji czy zdalnej kolaboracji na wspólnych dokumentach, bez istotnego zwiększenia zagrożenia dla bezpieczeństwa sieci i bez potrzeby dodatkowych nakładów inwestycyjnych na nową infrastrukturę i dodatkowe licencje.

Korzyści chmury wykraczają jednak daleko poza wygodę korzystania z aplikacji biurowych. Przedsiębiorstwa wdrażające chmurę uzyskują dostęp do dynamicznie skalowalnych zasobów obliczeniowych dostawcy, które mogą być wykorzystane m.in. w celu predykcji awarii, prognozowania zużycia i zapotrzebowania, prognozowania cen surowców, prowadzenia badań R&D związanych z analizą *big data* czy obliczeniami macierzowymi. W większości przypadków korzystanie z prawidłowo wdrożonej chmury pozwoli na obniżenie kosztów systemów IT, zwiększy szybkość i dostęp do danych, poprawi innowacyjność przedsiębiorstwa i poprawi bezpieczeństwo danych.

Aby w pełni wykorzystać potencjał tej technologii w polskiej energetyce, kluczowe jest jednak, aby polskie władze wydały dedykowane dla energetyki wytyczne o charakterze technicznym, prawnym i organizacyjnym, usuwające podstawowe wątpliwości uczestników rynku. Tego typu wytyczne mogą przyczynić się do zwiększenia pewności obrotu i ułatwić polskiej energetyce dalsze innowacje w oparciu o chmurę obliczeniową.



Instytut Jagielloński
ul. Marszałkowska 84/92 lok. 115
00-514 Warszawa

jagiellonski.pl
instytut@jagiellonski.pl