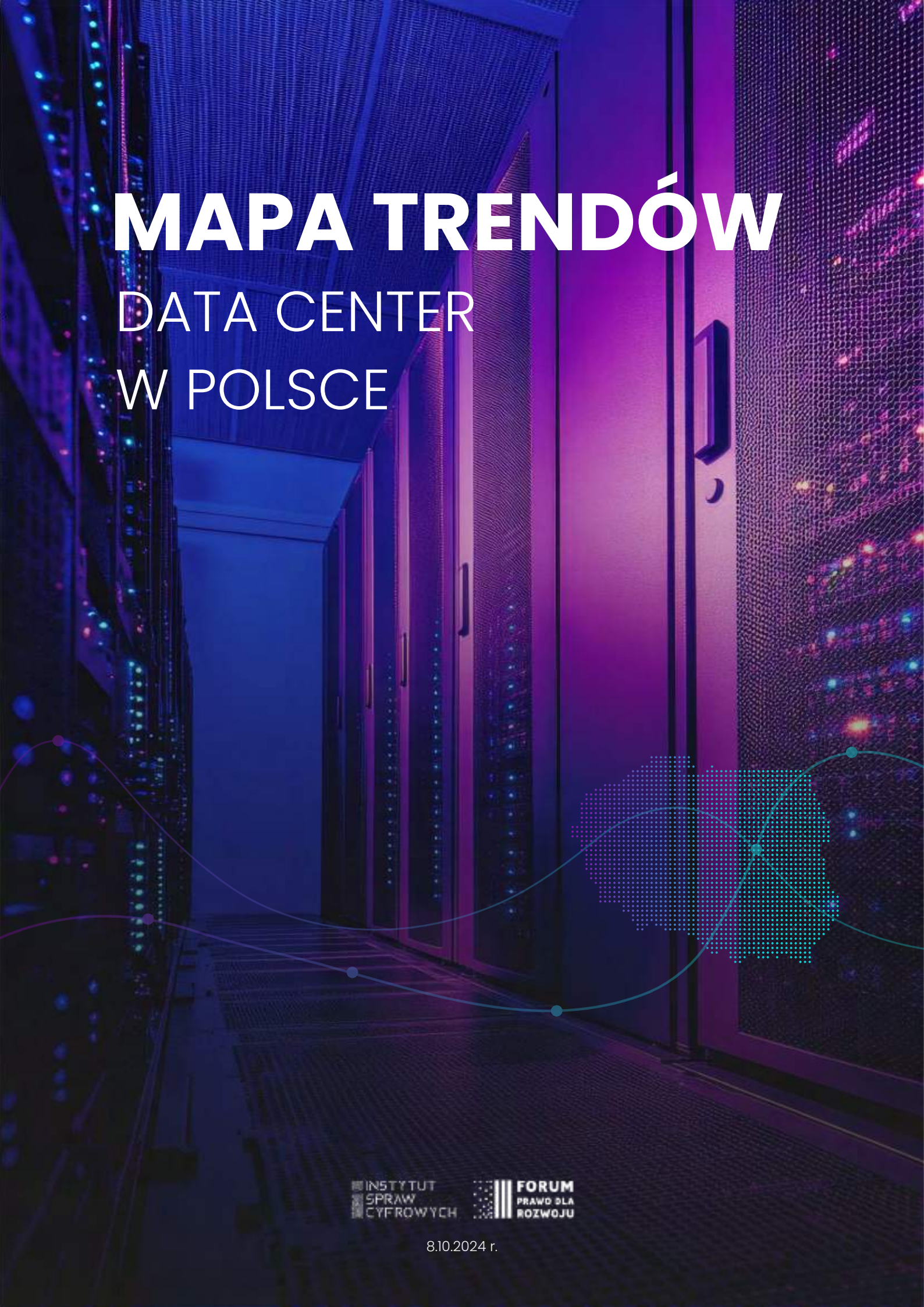


MAPA TRENDÓW

DATA CENTER W POLSCE

INSTYTUT SPRAW CYFROWYCH

FORUM PRAWO DLA ROZWOJU

8.10.2024 r.

MAPA TRENDÓW
DATA CENTER W POLSCE

SPIS TREŚCI

Spis treści

1. WPROWADZENIE

SŁOWO OD AUTORKI

Szanowni Państwo,

Z przyjemnością oddajemy w Państwa ręce raport „Mapa Trendów Data Center w Polsce", który powstał jako odpowiedź na dynamiczny rozwój tego sektora w naszym kraju. Przygotowany przez Instytut Spraw Cyfrowych we współpracy z Forum Prawo dla Rozwoju, raport ten stanowi kompleksowe kompendium wiedzy o bieżącym stanie rynku data center w Polsce, z uwzględnieniem kluczowych trendów, prognoz oraz rekomendacji dla firm.

Już w 2016 roku raport „Innowacyjna Cyfryzacja", przygotowany przez Krajową Izbę Gospodarczą Elektroniki i Telekomunikacji na zlecenie Ministerstwa Cyfryzacji, wskazywał na kluczową rolę rozwoju centrów danych w procesie cyfrowej transformacji Polski. Obecnie rosnące wymagania w zakresie zaawansowanych technologii, zrównoważonego rozwoju oraz innowacyjności stawiają przed firmami z sektora data center ogromne możliwości, ale także szereg wyzwań. Dostosowanie się do globalnych standardów i dynamicznie zmieniających się potrzeb rynku będzie kluczowym elementem budowania konkurencyjności polskiego sektora data center w najbliższych latach[1].

Celem niniejszego raportu jest nie tylko przedstawienie aktualnej sytuacji na rynku, lecz także zidentyfikowanie najważniejszych czynników kształtujących przyszłość tej branży. Podstawą naszych analiz były badania ankietowe przeprowadzone wśród firm korzystających z usług centrów danych, wywiady z ekspertami branżowymi, case studies, komentarze oraz szczegółowa analiza dostępnych danych rynkowych. Mamy nadzieję, że raport stanie się cennym źródłem wiedzy dla przedsiębiorstw, inwestorów, decydentów oraz wszystkich zainteresowanych rozwojem rynku data center w Polsce i zainspiruje do podejmowania działań, które przyniosą korzyści całej gospodarce cyfrowej w naszym kraju.

Z poważaniem,
Kamila Pendyk
Prezeska Instytutu Spraw Cyfrowych

Kamila Pendyk
Instytut Spraw Cyfrowych

[1] https://kigeit.org.pl/FTP/Raporty/Innowacyjna_Cyfryzacja.pdf

1A. ZAKRES BADAŃ

Raport opiera się na zróżnicowanych metodach zbierania danych, w tym ankietach wśród firm korzystających z usług centrów danych, wywiadach z ekspertami branżowymi, analizie przypadków wdrożeń (case studies) oraz analizie desk research. Badanie miało na celu zrozumienie preferencji klientów, ich oczekiwań wobec dostawców usług data center oraz zidentyfikowanie kluczowych trendów rynkowych. Raport zawiera również przegląd historycznego rozwoju rynku data center w Polsce, opisuje jego obecny stan oraz porównuje polski rynek z europejskim i światowym. Analizuje również obecne przepisy prawne i regulacje, które kształtują działanie centrów danych, w tym kwestie ochrony danych osobowych, bezpieczeństwa informacji, regulacji rządowych i ochrony przed cyberatakami.
Raport zawiera głębokie zrozumienie kierunków technologicznych, ekologicznych, ekonomicznych, bezpieczeństwa i regulacyjnych, które kształtują branżę data center. Równocześnie zawiera rekomendacje dla firm działających w tej branży oraz wskazuje strategiczne kroki, które mogą zostać podjęte w odpowiedzi na zidentyfikowane trendy.

1B. KLUCZOWE WNIOSKI

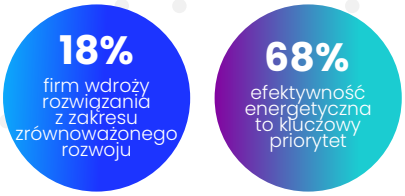
W Polsce działa obecnie 112 data center o łącznej mocy 200 MW, ale tylko 65 z nich zajmuje ponad 200 m². Polska należy do grona rynków potencjalnego wzrostu, określanych jako Tier II. W kolejnych dwóch latach nastąpi dynamiczny przyrost mocy wraz z inwestycjami Microsoft, Atman, Data4 i Krajowego Centrum Przetwarzania Danych. Kluczowym wyzwaniem dla wyżej wymienionych jak również potencjalnych kolejnych inwestycji jest dostępność energii elektrycznej. Równolegle sektor podlega pięciu głównym trendom zmian:

1. Technologiczne:

- **Dominacja chmury (Cloud Dominance Era):** Chmura obliczeniowa stała się kluczowym elementem infrastruktury IT w polskich firmach. **78%** respondentów korzysta z chmury, a usługi PaaS i SaaS zyskują na popularności, wskazując na potrzebę elastycznych i wydajnych rozwiązań.
- **Transformacja AI (Intelligence-Driven Transformation):** Coraz więcej firm **(64%)** planuje wdrożenie technologii sztucznej inteligencji i uczenia maszynowego. Dostawcy usług data center muszą być przygotowani do obsługi tych zaawansowanych technologii i oferować infrastrukturę wspierającą inicjatywy cyfrowej transformacji.
- **Rewolucja kwantowa (Quantum Data Revolution): 50%** respondentów rozważa integrację technologii kwantowych, co oznacza konieczność inwestycji w rozwój infrastruktury kwantowej oraz przygotowanie do nowych standardów bezpieczeństwa.

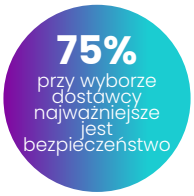
2. Ekologiczne

- **Niski poziom eko-świadomości (Low Eco):** W pytaniu dotyczącym planowanych w przyszłości inwestycji w data center w perspektywie 3-5 lat tylko **18%** firm wskazało wdrażanie rozwiązań z zakresu zrównoważonego rozwoju. Rząd i branża powinni podjąć działania edukacyjne w celu zwiększenia świadomości w zakresie green IT.
- **Priorytet energii (Rule of Energy):** Efektywność energetyczna jest kluczowym priorytetem dla **68%** respondentów. Firmy kładą nacisk na optymalizację zużycia energii oraz redukcję emisji CO2, co wpływa zarówno na koszty operacyjne, jak i na reputację.



3. Bezpieczeństwa:

- **Bezpieczeństwo ponad wszystko (Safety First):** Bezpieczeństwo danych jest najważniejszym kryterium przy wyborze dostawcy usług centrów danych dla **75%** respondentów. Firmy muszą inwestować w zaawansowane strategie cyberbezpieczeństwa oraz zabezpieczenia fizyczne obiektów.
- **Powrót do fundamentów (Back to Basics):** Rosnąca potrzeba modernizacji istniejącej infrastruktury wskazuje na konieczność skupienia się na solidnych fundamentach, umożliwiających przyszłe wdrażanie zaawansowanych technologii.



4. Ekonomiczne:

- **Czas subskrypcji (Subscription Time):** Rosnące zainteresowanie modelem subskrypcyjnym w opłatach za usługi infrastruktury IT (**55%** respondentów) wskazuje na potrzebę oferowania elastycznych pakietów usług.
- **Elastyczność kosztów (Flexible Cost Evolution):** Firmy inwestują w modernizację infrastruktury i usługi chmurowe, aby zapewnić elastyczność operacyjną i dostosowywać zasoby do zmieniających się potrzeb.

5. Regulacyjne:

- **Eko-Prawo (Environmental Law):** Nowe regulacje, takie jak planowane wprowadzenie ETS 2 w 2027 roku, wpłyną na sektor data center, wymuszając dostosowanie do wyższych standardów efektywności energetycznej.
- **Relokalizacja (Go Local):** Rosnące wymagania dotyczące lokalizacji danych, zarówno w Polsce, jak i w innych krajach, skłaniają operatorów centrów danych do inwestowania w lokalną infrastrukturę. Jest to nie tylko odpowiedź na przepisy o ochronie danych, ale także strategia zapewniająca zgodność z różnorodnymi wymogami prawnymi.
- **Era NIS (NIS Era):** Nowe regulacje w zakresie cyberbezpieczeństwa, takie jak dyrektywa NIS 2, zaczną kształtować strategie zarządzania danymi. Firmy będą musiały inwestować w zaawansowane środki bezpieczeństwa, aby sprostać rosnącym wymaganiom dotyczącym ochrony sieci i systemów informatycznych.
- **REIT centrów danych (Data Center REIT):** Rozwój rynku nieruchomości inwestycyjnych w sektorze centrów danych poprzez REIT (Real Estate Investment Trust) może otworzyć nowe możliwości finansowania. Choć to rozwiązanie jest wciąż w początkowej fazie w Polsce, jego rozwój w przyszłości może znacząco wpłynąć na strategię inwestycyjną w branży data center.

Przewidywania i wyzwania

Branża centrów danych odpowiada za około 4% światowego zużycia energii elektrycznej. Do tej pory standardowe centra danych były budowane na działkach o powierzchni 4-6 ha, z mocą na poziomie 30-60 MW. W przypadku obiektów przeznaczonych do obsługi sztucznej inteligencji, wielkość działki może być nawet o połowę mniejsza, jednak zapotrzebowanie na moc rośnie dwukrotnie, osiągając nawet 120 MW. W kontekście obecnego, przeciążonego systemu energetycznego stanowi to ogromne wyzwanie. Dokładając do tego fakt, że mamy wPolsce jedne z najwyższych cen energii na świecie, **potrzebujemy odpowiednich polityk**

i regulacji, które pozwolą na zapewnienie odpowiedniej ilości zielonej energii oraz gruntów pod wzrost sektora centrów danych w synergii z nowymi źródłami energii.
Alternatywną strategią mogłaby być technologiczna ucieczka do przodu poprzez wczesne wprowadzenie rozwiązań kwantowych. Szacuje się, że komputery kwantowe mogą zużywać nawet sto razy mniej energii niż najnowocześniejsze superkomputery, osiągając podobne czasy przetwarzania. **Wykorzystanie obliczeń kwantowych może znacząco usprawnić zarządzanie energią w czasie rzeczywistym, co jest kluczowe dla optymalizacji jej zużycia w dużych centrach danych.** Dzięki szybszemu przetwarzaniu informacji, optymalizacji algorytmów, zmniejszeniu liczby operacji oraz zaawansowanym symulacjom i modelowaniu kwantowemu, możliwe stanie się efektywniejsze planowanie i kontrola zasobów energetycznych. **Tego rodzaju strategia właściwa jest gospodarkom rozwiniętym, stąd nie powinno dziwić, iż nie widać dzisiaj w Polsce predykatów dających nadzieję na możliwość jej adopcji.**

W obliczu wyzwań kryjących się w trendach technologicznych, ekonomicznych, ekologicznych, bezpieczeństwa i regulacyjnych, to w szczególności same firmy z sektora data center muszą szukać nowatorskich rozwiązań, które przyniosą długoterminowe korzyści.

Wykorzystanie obliczeń kwantowych może znacząco usprawnić zarządzanie energią w czasie rzeczywistym, co jest kluczowe dla optymalizacji jej zużycia w dużych centrach danych.

Integracja zielonej energii (takiej jak OZE czy małe reaktory modułowe – SMR) z infrastrukturą data center może przynieść znaczące korzyści zarówno ekonomiczne, jak i ekologiczne. Umieszczenie farm fotowoltaicznych, biogazowni, turbin wiatrowych lub innych źródeł OZE, czy też SMR w sąsiedztwie centrum danych, pozwoliłoby na bezpośrednie wykorzystanie produkowanej energii (a w przypadku SMR lub ich integracji ze spalaniem biogazu również zapewnienia ciągłości działania). Taka strategia nie tylko obniżyłaby koszty operacyjne związane z zasilaniem i chłodzeniem, ale także zredukowałaby ślad węglowy, odpowiadając na rosnące wymagania dotyczące zrównoważonego rozwoju.

Drugim elementem tej synergii jest **wykorzystanie ciepła odpadowego generowanego przez centra danych.** Wytwarzane w procesie chłodzenia ogromne ilości ciepła mogą być efektywnie wykorzystane do ogrzewania pobliskich budynków a nawet większych obszarów miejskich.

Wprowadzenie tego typu rozwiązań pozwoliłoby data center pełnić ważną rolę w lokalnych systemach energetycznych, zwiększając efektywność energetyczną na poziomie całego miasta. Takie rozwiązania już funkcjonują: Meta w Odense (Dania), AWS w Dublinie (Irlandia) oraz Microsoft w Espoo i Kirkkonummi (Finlandia).

Synergia między data center a zieloną infrastrukturą energetyczną stanowi zatem nie tylko inwestycję w przyszłość sektora, ale także w zrównoważony rozwój gospodarki i społeczeństwa. Tego rodzaju inicjatywy integrują data center z miejską infrastrukturą, przynosząc jednocześnie korzyści społeczne i środowiskowe.

Dążenie do połączenia technologii, zrównoważonego rozwoju i efektywności ekonomicznej może stać się kluczowym czynnikiem konkurencyjności na rynku i katalizatorem dla przyspieszenia cyfrowej transformacji w Polsce.

2. MAPA TRENDÓW

2.1. GRAFICZNE PRZEDSTAWIENIE TRENDÓW

2.2. OPIS KAŻDEGO ZIDENTYFIKOWANEGO TRENDU

2.2.1. TECHNOLOGICZNE

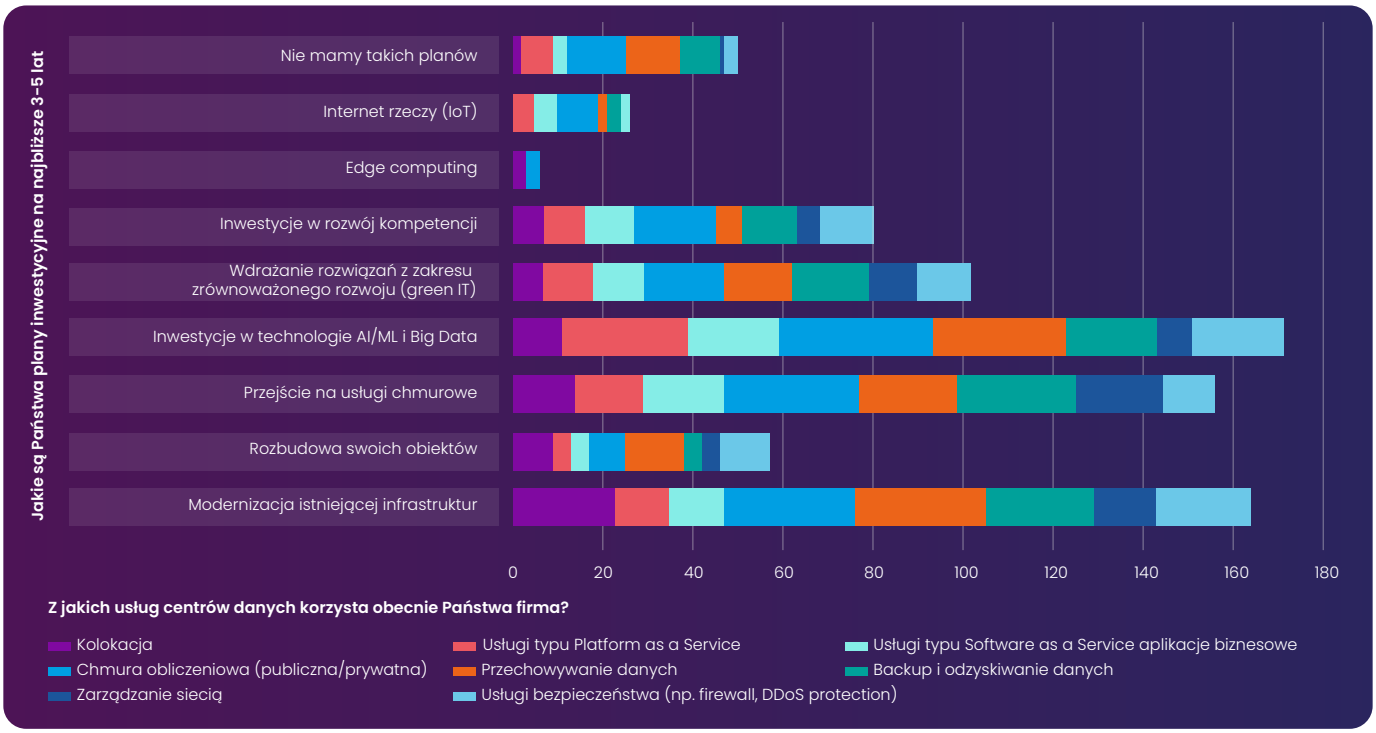
1. Cloud Dominance Era / Dominacja chmury

78% „chmura to kluczowy element infrastruktury"

Rosnąca adopcja chmury: Chmura obliczeniowa stała się kluczowym elementem infrastruktury IT w firmach, a jej wykorzystywanie wskazuje **78%** respondentów (zarówno jeśli chodzi o chmurę publiczną, jak i prywatną). Trend ten odzwierciedla rosnące zapotrzebowanie na elastyczne, skalowalne i wydajne rozwiązania, które mogą wspierać dynamiczne zmiany w środowisku biznesowym. Chmura umożliwia firmom szybkie reagowanie na zmieniające się potrzeby, optymalizację kosztów oraz zwiększenie dostępności usług.

Zróżnicowanie usług chmurowych: Usługi typu Platform as a Service (PaaS) i Software as a Service (SaaS) również zyskują na popularności, z odpowiednio **45% i 37%** firm korzystających z tych rozwiązań. PaaS umożliwia firmom rozwijanie aplikacji bez konieczności zarządzania infrastrukturą, co przyspiesza procesy deweloperskie. SaaS z kolei oferuje gotowe do użycia aplikacje, co zmniejsza potrzebę wewnętrznego utrzymywania i zarządzania oprogramowaniem.

45% PaaS **37%** SaaS



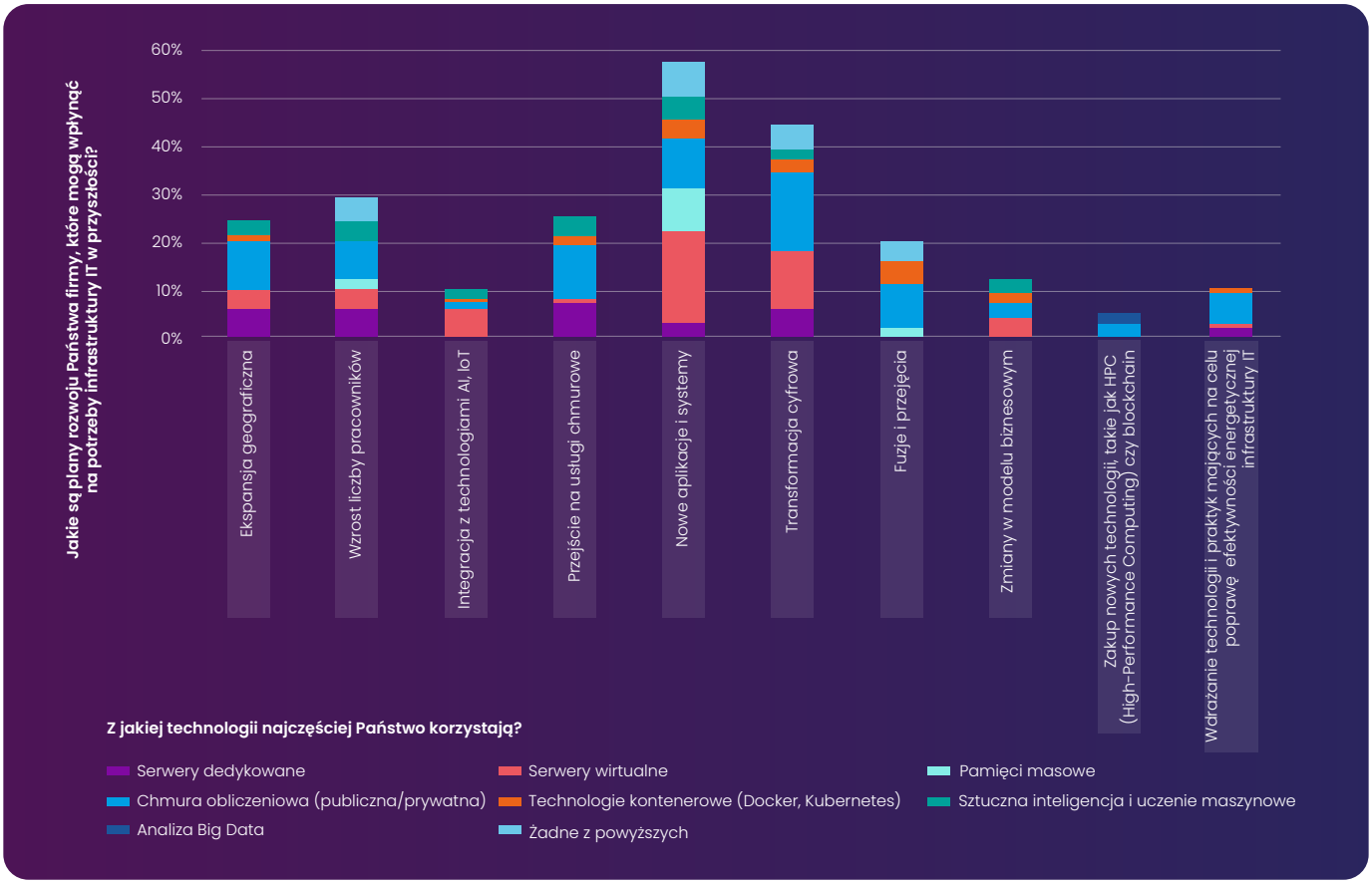
2. INTELLIGENCE-DRIVEN TRANSFORMATION / TRANSFORMACJA AI

Firmy coraz bardziej dostrzegają znaczenie integracji AI i IoT z ich obecną infrastrukturą IT, szczególnie wykorzystując serwery wirtualne i chmurę obliczeniową jako kluczowe platformy. Trend ten pokazuje silne zainteresowanie wykorzystaniem usług chmurowych i środowisk wirtualnych do wsparcia inicjatyw transformacji cyfrowej, z AI w centrum tych planów. Widoczny jest także nacisk na rozwijanie nowych aplikacji korzystających z AI, co wskazuje na przejście w kierunku bardziej inteligentnych i zautomatyzowanych systemów.

64% firm planuje wdrożenie technologii AI/ML

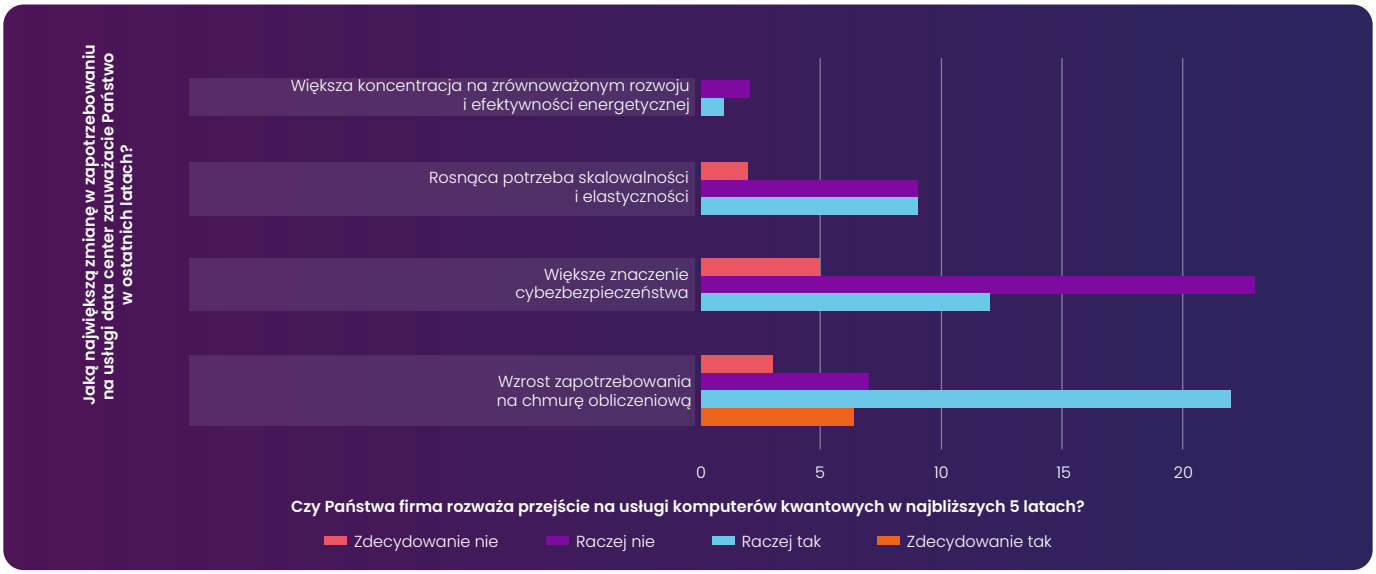
Dane wskazują, że dążenie do integracji i wykorzystania AI w infrastrukturze IT kształtuje strategie firm, sugerując silny ruch w kierunku cyfrowej transformacji opartej na AI w najbliższej przyszłości.

Warto podkreślić, że **64%** firm planuje wdrożenie technologii AI/ML w najbliższych 3-5 lat. Świadczy to o rosnącym zainteresowaniu automatyzacją oraz analizą danych, które mogą przynieść znaczące korzyści w zakresie optymalizacji kosztów, efektywności operacyjnej oraz przewagi konkurencyjnej.



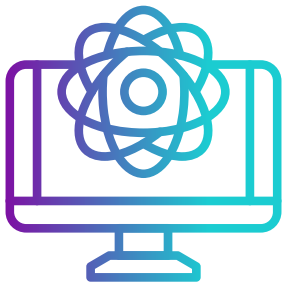
3. QUANTUM DATA REVOLUTION / REWOLUCJA KWANTOWA

Łącznie aż 50% respondentów wskazuje, że rozważa przejście na usługi komputerów kwantowych w ciągu najbliższych 5 lat, w tym 6% z nich zdecydowanie planuje taki krok (odpowiedzi zdecydowanie tak). Pokazuje to, że firmy przygotowują się na współistnienie tradycyjnych i kwantowych rozwiązań, takich jak chmura obliczeniowa czy kolokacja, oraz na oferowanie zdalnego dostępu do technologii kwantowych. Analiza ankiet wskazuje na znaczące zainteresowanie firm przejściem na komputery kwantowe, co potwierdzają też wnioski z wywiadu z Panią Anną Streżyńską.



Związek między wzrostem zapotrzebowania na chmurę obliczeniową a rozważaniem przejścia na usługi komputerów kwantowych. Wzrost zapotrzebowania na chmurę obliczeniową był zauważalny głównie wśród firm, które jednocześnie rozważają przejście na usługi komputerów kwantowych.

Cyberbezpieczeństwo a usługi komputerów kwantowych. Firmy, które zaznaczyły "raczej nie" (41%) oraz "zdecydowanie nie" (10%) w odpowiedzi na pytanie o chęć przejścia na usługi komputerów kwantowych, zwracały większą uwagę na znaczenie cyberbezpieczeństwa. Może to sugerować, że te firmy postrzegają wyzwania związane z cyberbezpieczeństwem jako bardziej pilne niż wdrażanie nowych technologii, takich jak komputery kwantowe.



Zwiększona wydajność i szybkość przetwarzania danych: Komputery kwantowe oferują ogromny potencjał przyspieszenia procesów przetwarzania danych, szczególnie w analizie dużych zbiorów danych i rozwiązywaniu skomplikowanych problemów. Szybkość przetwarzania dzięki superpozycji i splątaniu kwantowemu może zrewolucjonizować branżę, umożliwiając szybszy dostęp do informacji.

Nowe standardy szyfrowania i bezpieczeństwa: Quantum computing znacząco wpłynie na bezpieczeństwo danych w centrach danych. Wprowadzenie kwantowej kryptografii i algorytmów odpornych na ataki kwantowe zapewni wyższy poziom ochrony danych. Technologia Quantum Key Distribution (QKD) pozwoli na bezpieczne przekazywanie kluczy szyfrujących, eliminując ryzyko podsłuchu.

Rozwój regulacji i standaryzacji technologii kwantowych: Z uwagi na specyficzne wymagania technologii kwantowej, niezbędne będą nowe regulacje i standardy dotyczące zasilania, chłodzenia, zarządzania kablami oraz bezpieczeństwa. Branża będzie musiała współpracować z organizacjami standaryzacyjnymi, takimi jak ISO, ITU i IEEE, aby stworzyć jednolite ramy dla integracji technologii kwantowych z tradycyjnymi systemami.

Zastosowania w AI i uczeniu maszynowym: Quantum computing znacznie przyspieszy algorytmy sztucznej inteligencji (AI) i uczenia maszynowego (ML), co zwiększy możliwości analizy dużych zbiorów danych oraz poprawi wydajność operacyjną centrów danych. Kwantowe algorytmy umożliwią bardziej zaawansowane rozpoznawanie wzorców i podejmowanie decyzji w czasie rzeczywistym.

Współpraca operatorów centrów danych i producentów komputerów kwantowych: Kluczowa będzie ścisła współpraca między operatorami centrów danych a producentami komputerów kwantowych, aby zapewnić efektywną integrację technologii oraz rozwój badań i innowacji w tym zakresie.

Zmniejszenie zużycia energii i optymalizacja chłodzenia:

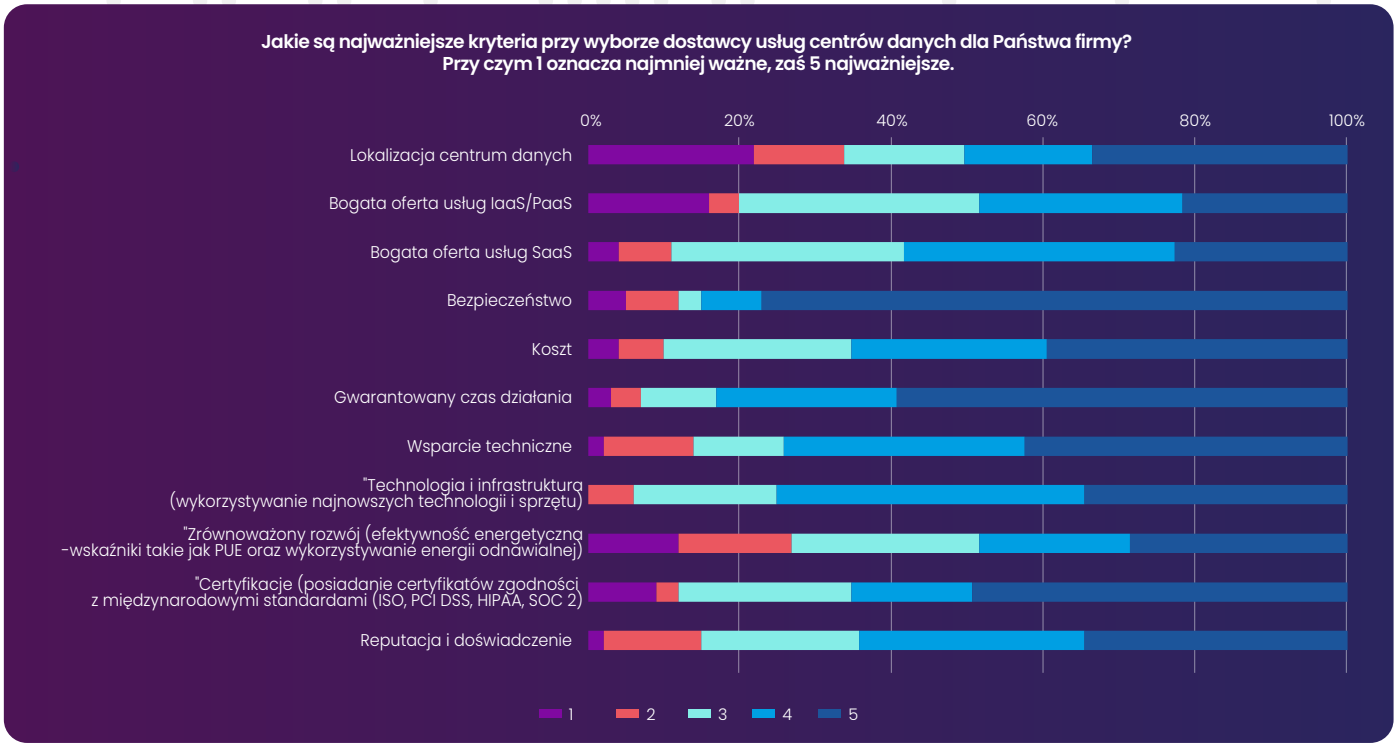
Obliczenia kwantowe zużywają znacznie mniej energii niż tradycyjne superkomputery, co może prowadzić do znacznej redukcji zapotrzebowania na energię w centrach danych. Dodatkowo, technologie kwantowe mogą optymalizować zarządzanie ciepłem, co przyczyni się do oszczędności energii i wody wykorzystywanej w systemach chłodzenia.

2.2.2. EKOLOGICZNE

1. LOW ECO / MNIEJ EKO-ŚWIADOMOŚCI

Zaangażowanie dużych firm w inicjatywy proekologiczne, w ramach prowadzonych przez nie działań PR, mogłoby sugerować rosnącą świadomość przedsiębiorstw na całym świecie w zakresie zrównoważonego rozwoju. Jednocześnie, odpowiedzi respondentów na pytanie dotyczące kryteriów wyboru dostawcy data center oraz planów inwestycyjnych na najbliższe 3-5 lat pokazuje odmienny obraz polskich firm. Tylko **18%** respondentów wskazało na wdrażanie rozwiązań z zakresu zrównoważonego rozwoju (green IT). W pytaniu o kryteria wyboru dostawcy usług data center, zrównoważony rozwój zajął dopiero dziewiąte miejsce na jedenaście możliwych.

18% planuje wdrożenie rozwiązań green IT



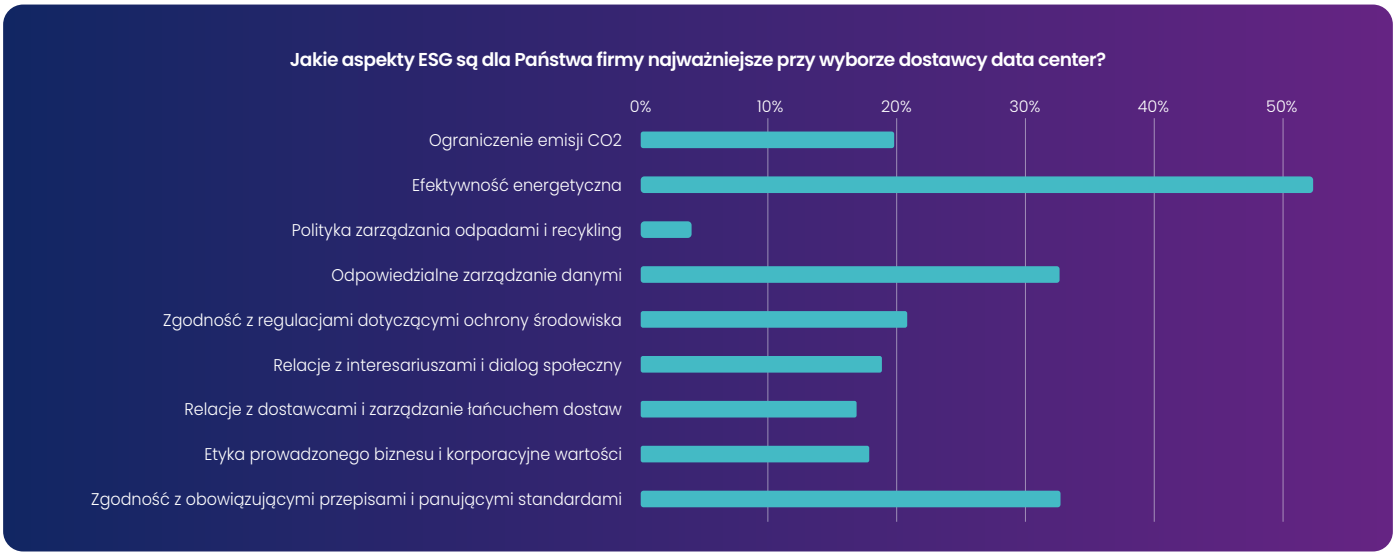
2. RULE OF ENERGY / PRIORYTET ENERGII

Efektywność energetyczna została wskazana jako najważniejszy trend ekologiczny przez **68%** respondentów. Firmy kładą duży nacisk na optymalizację zużycia energii, co ma bezpośredni wpływ na zmniejszenie kosztów operacyjnych oraz redukcję emisji CO_2.

Poprawa efektywności energetycznej w centrach danych przynosi znaczące oszczędności finansowe. Inwestycje w nowoczesne systemy chłodzenia, czy technologie pozwalające na lepsze zarządzanie zasobami, zwracają się w postaci niższych rachunków za energię. Firmy, które priorytetowo traktują efektywność energetyczną, zyskują także reputację odpowiedzialnych i ekologicznych partnerów biznesowych.

52% podczas wyboru dostawcy efektywność energetyczna jest najważniejsza

Ponad połowa respondentów zapytana o aspekty ESG, które są najważniejsze przy wyborze dostawcy data center wskazała na efektywność energetyczną **(52%)**. Pozostałe możliwe odpowiedzi to: ograniczenie emisji CO_2, polityki zarządzania odpadami, odpowiedzialnym zarządzaniem danymi czy zgodności z regulacjami czy etyką.



2.2.3. BEZPIECZEŃSTWA

1. SAFETY FIRST / BEZPIECZEŃSTWO PONAD WSZYSTKO

4,46 bezpieczeństwo najważniejszym kryterium przy wyborze dostawcy

Bezpieczeństwo jest najważniejszym kryterium przy wyborze dostawcy usług data center - z oceną **4,46 (w skali 1 do 5)**. Respondenci wskazali bezpieczeństwo jako kluczowy czynnik, co pokazuje, że firmy przykładają coraz większą wagę do ochrony swoich danych i infrastruktury. Trendy związane z bezpieczeństwem w centrach danych wyłaniające się z ankiety wskazują na kluczową rolę, jaką ochrona danych i infrastruktury odgrywa w strategiach firm. Z rosnącą cyfryzacją i coraz bardziej złożonymi zagrożeniami cybernetycznymi, firmy kładą coraz większy nacisk na rozwój kompleksowych strategii bezpieczeństwa.

2. BACK TO BASICS / POWRÓT DO FUNDAMENTÓW

Ostatnimi czasy skupialiśmy się głównie na dynamicznym rozwoju technologii, a teraz widoczny jest **trend powrotu do fundamentów – przyglądania się przestarzałej infrastrukturze i przygotowywania jej na jeszcze większy rozwój, w tym potencjalnie na technologie takie jak komputery kwantowe.** Aby jednak móc się dalej rozwijać, konieczne jest posiadanie solidnych podstaw, do których firmy obecnie dążą.

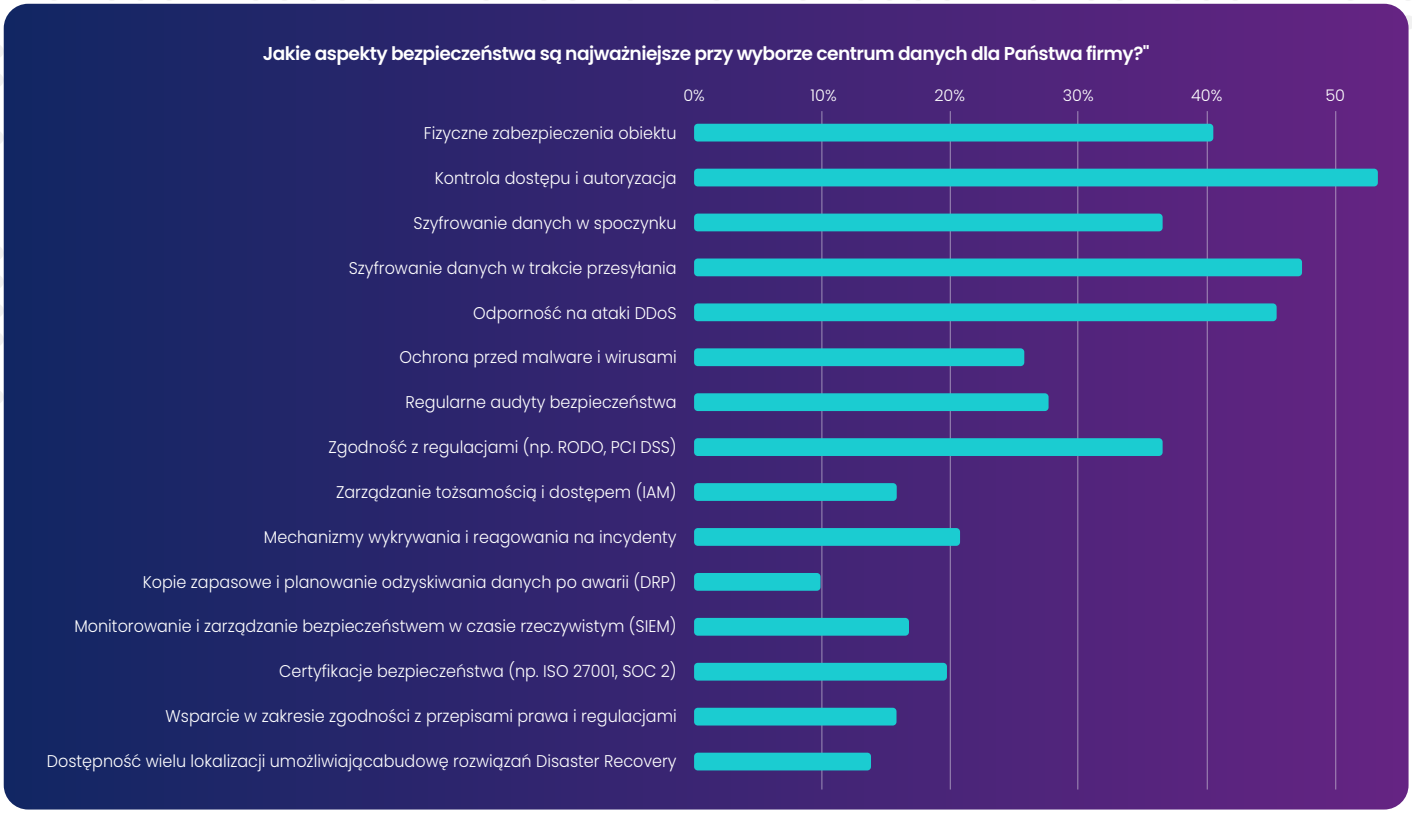
41% ochrona fizyczna obiektów jest ważna przy wyborze centrum danych

Ochrona fizyczna obiektów data center, kontrola dostępu i monitoring oraz bariery fizyczne, zostały wskazane przez respondentów jako najważniejsze aspekty przy wyborze centrum danych (kolejno: **41%, 53% i 17%**).

Fizyczne zabezpieczenia zapewniają, że dostęp do krytycznych zasobów jest ściśle kontrolowany i monitorowany, co minimalizuje ryzyko fizycznego sabotażu lub nieautoryzowanego dostępu.

Modernizacja istniejącej infrastruktury to drugi najczęściej wskazywany obszar planowanych inwestycji na najbliższe 3-5 lat w zakresie data center **(40%)**. Więcej wskazań uzyskały jedynie inwestycje w technologie AI **(42%)**. Sytuacja ta wskazuje, że po okresie intensywnych nakładów na rozwój nowych technologii, obserwujemy nieustającą transformację cyfrową, a firmy zaczynają wracać do podstaw, takich jak **inwestycje w infrastrukturę oraz zabezpieczenia fizyczne.**

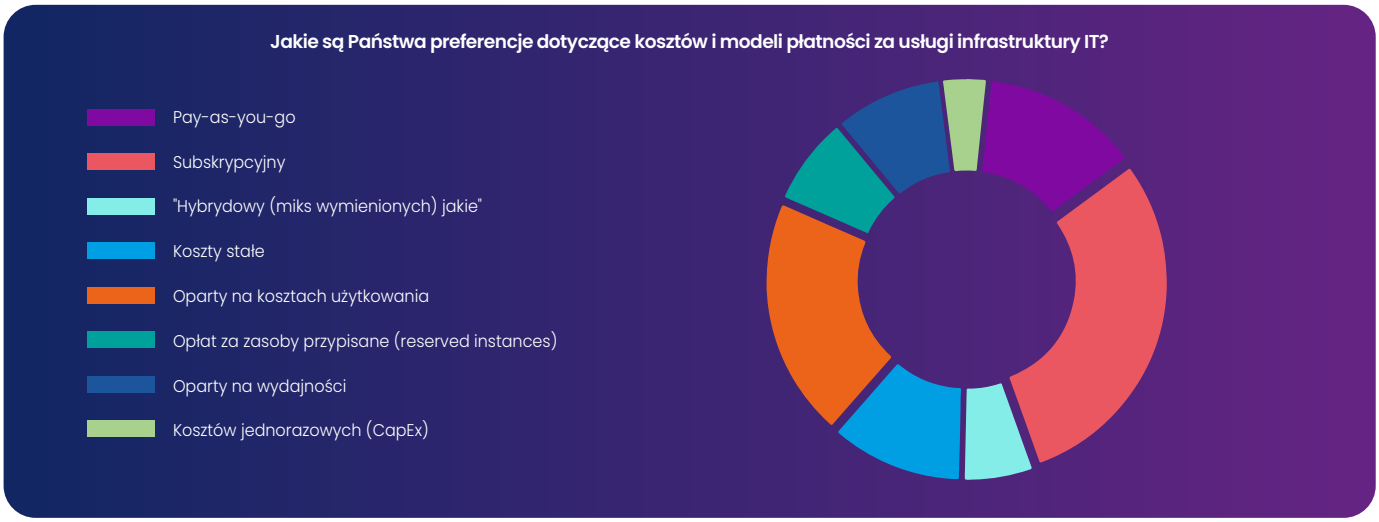
42% planuje inwestycje w technologie AI w ciągu 3-5 lat



2.2.4. EKONOMICZNE

1. SUBSCRIPTION TIME / CZAS SUBSKRYPCJI

Z odpowiedzi respondentów wyłania się wyraźny trend preferowania modelu subskrypcyjnego w opłatach za usługi infrastruktury IT, co potwierdziło **55%** ankietowanych. Wybór ten wskazuje na zmieniające się podejście firm do zarządzania infrastrukturą IT oraz budżetowaniem wydatków na te usługi.
Rosnące zainteresowanie modelem subskrypcyjnym może sugerować, że **w przyszłości coraz więcej dostawców usług data center oraz infrastruktury IT będzie wprowadzać lub rozszerzać swoje oferty subskrypcyjne,** dostosowując je do dynamicznych potrzeb firm. W obliczu postępującej digitalizacji i konieczności szybkiego dostosowywania się do zmian, firmy będą preferowały modele płatności, które pozwolą im na elastyczne zarządzanie technologią i kosztami operacyjnymi.



2. FLEXIBLE COST EVOLUTION / ELASTYCZNOŚĆ KOSZTÓW

W obliczu różnorodnych planów rozwoju, takich jak ekspansja geograficzna, transformacja cyfrowa czy wdrażanie nowych technologii, firmy coraz częściej stawiają na strategie, które pozwalają na elastyczne zarządzanie kosztami. Wdrażanie rozwiązań zapewniających zgodność z regulacjami, niezawodność systemów, bezpieczeństwo fizyczne i cybernetyczne, a także optymalizację efektywności energetycznej, wskazuje na potrzebę inwestycji w infrastrukturę, która jest skalowalna, bezpieczna i zgodna z dynamicznie zmieniającym się otoczeniem biznesowym.

Dzięki takiemu podejściu firmy są w stanie dostosowywać swoje wydatki operacyjne do bieżących potrzeb, minimalizować ryzyko finansowe i wykorzystywać nowe technologie w sposób bardziej elastyczny.

2.2.5 REGULACYJNE

1. ENVIRONMENTAL LAW / EKO-PRAWO

Zrównoważony Rozwój i Efektywność Energetyczna

Rafał Kittel
Kancelaria KJW

W obliczu rosnącej świadomości ekologicznej i globalnych wyzwań związanych z klimatem, wiele krajów na całym świecie wprowadza nowe regulacje mające na celu ograniczenie emisji dwutlenku węgla (CO_2). Ze względu na globalną skalę problemu, działania te podejmowane są niejednokrotnie nie jedynie samodzielnie na szczeblu poszczególnych państw, ale na poziomie międzynarodowych umów lub rozwiązań przyjmowanych przez organizacje państw. M.in. w Unii Europejskiej, dyrektywy klimatyczne i energetyczne, takie jak Europejski Zielony Ład, wyznaczają ambitne cele redukcji emisji gazów cieplarnianych.

Od 2027 roku operacyjnym stanie się tzw. ETS 2 (skrót od: Emissions Trading System 2). Będzie to nowy, obowiązujący na terytorium Unii Europejskiej system handlu uprawnieniami do emisji, odrębny od istniejącego obecnie EU ETS (European Union Emissions Trading System).

Ten nowy system, wprowadzony na mocy Dyrektywy Parlamentu Europejskiego i Rady (UE) 2023/959 z dnia 10 maja 2023 r. zmieniającej dyrektywę 2003/87/WE ustanawiającą system handlu przydziałami emisji gazów cieplarnianych w Unii oraz decyzję (UE) 2015/1814 w sprawie ustanowienia i funkcjonowania rezerwy stabilności rynkowej dla unijnego systemu handlu uprawnieniami do emisji gazów cieplarnianych, obejmie emisje CO_2 ze spalania paliw w budynkach, transporcie drogowym i w dodatkowych sektorach (głównie w małym przemyśle nieobjętym istniejącym EU ETS) oraz zajmie się tymi emisjami[1].

Chociaż formalnie, nowy system obowiązywał będzie wyłącznie podmioty wskazane w ww. dyrektywie, zobowiązane do nabywania i umarzania swoich uprawnień do emisji CO_2, to w ramach rozwiązań przyjmowanych w poszczególnych państwach członkowskich, nowe obciążenia, szczególnie fiskalne, mogą objąć również końcowych użytkowników, takich jak np. właściciele budynków, czy też operatorzy centrów danych. Stają więc oni, podobnie jak wytwórcy konsumowanej przez ich firmy energii, przed wyzwaniem, które wymaga wdrożenia zaawansowanych technologii zwiększających efektywność energetyczną oraz korzystania z odnawialnych źródeł energii.

Centra danych, będące sercem infrastruktury cyfrowej, są jednocześnie dużymi konsumentami energii. Według Międzynarodowej Agencji Energetycznej (IEA)

w 2021 r. centra danych odpowiadały za zużycie 220-320 TWh energii, co stanowiło wówczas około 1% całkowitego zapotrzebowania na energię elektryczną na świecie[2]

Wg. danych z roku 2023, obecne zużycie szacuje się już na 1 – 1,5 % światowego zużycia. W miarę jak globalne zapotrzebowanie na przetwarzanie danych rośnie, rośnie również energochłonność centrum danych i towarzysząca jej emisja CO_2.

Dostosowanie się do takich warunków, wymaga od operatorów centrów danych przemyślenia strategii zarządzania energią. Ponieważ operatorzy nie zawsze mogą w całości lub w części przejść na zasilanie z odnawialnych źródeł energii, zwiększenie efektywności energetycznej staje się kluczowym aspektem. W praktyce oznacza to modernizację infrastruktury IT, optymalizację systemów chłodzenia oraz korzystanie z bardziej efektywnych technologii przetwarzania danych.

Proces ten można połączyć z ubieganiem się o jeden z certyfikatów ekologicznych. Nie tylko pozwoli to skorzystać z opracowanej i skutecznej ścieżki przejścia do modelu efektywnego i energooszczędnego zasilania, ale gwarantuje możliwość udokumentowania sukcesu w tym zakresie.

Certyfikaty takie jak LEED (Leadership in Energy and Environmental Design), BREEAM (Building Research Establishment Environmental Assessment Method) oraz Green Globes stają się pożądane w branży centrów danych, jako dowód na zgodność z wysokimi standardami zrównoważonego rozwoju.

1. LEED

W obliczu rosnącej świadomości ekologicznej i globalnych wyzwań związanych z klimatem, wiele krajów na całym świecie wprowadza nowe regulacje mające na celu ograniczenie emisji dwutlenku węgla (CO_2). Ze względu na globalną skalę problemu, działania te podejmowane są niejednokrotnie nie jedynie samodzielnie na szczeblu poszczególnych państw, ale na poziomie międzynarodowych umów lub rozwiązań przyjmowanych przez organizacje państw. M.in. w Unii Europejskiej, dyrektywy klimatyczne i energetyczne, takie jak Europejski Zielony Ład, wyznaczają ambitne cele redukcji emisji gazów cieplarnianych.

2. BREEAM

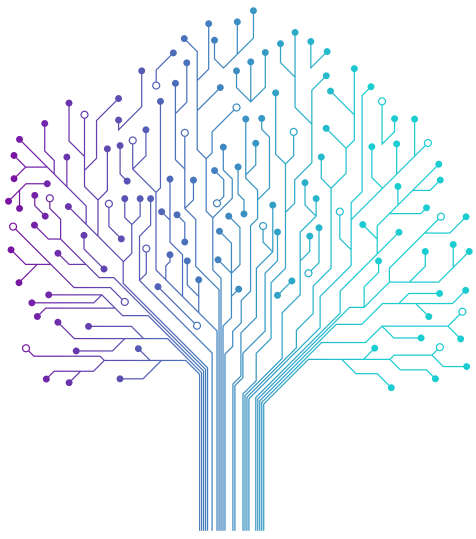
BREEAM, jako europejski odpowiednik LEED, również stawia wysokie wymagania w zakresie zrównoważonego rozwoju. Certyfikacja BREEAM ocenia budynki na podstawie takich kryteriów jak zarządzanie energią, użycie ekologicznych materiałów, zarządzanie odpadami, jakość powietrza oraz wpływ na środowisko naturalne. Dla centrów danych, uzyskanie certyfikatu BREEAM jest nie tylko potwierdzeniem dbałości o środowisko, ale również sposobem na zademonstrowanie zaangażowania w zrównoważony rozwój na globalnym rynku.

3. Green Globes

Green Globes, mniej znany w Europie, ale popularny w Ameryce Północnej, jest kolejnym systemem oceny ekologicznej, który oferuje elastyczne podejście do certyfikacji budynków. System ten koncentruje się na zrównoważonym zarządzaniu energią, zużyciu wody, zarządzaniu materiałami oraz optymalizacji kosztów operacyjnych. Dla centrów danych, które dążą do uzyskania certyfikatu Green Globes, kluczowe jest zrozumienie i integracja tych kryteriów na każdym etapie planowania i budowy.

Uzyskanie certyfikatów ekologicznych, takich jak LEED, BREEAM czy Green Globes, wiąże się z dodatkowymi kosztami, zarówno na etapie projektowania, jak i budowy centrów danych. Wymagania dotyczące zastosowania bardziej efektywnych materiałów, zaawansowanych technologii energetycznych oraz zarządzania zasobami naturalnymi mogą znacznie podnieść koszty inwestycji. Dodatkowo, proces certyfikacji jest czasochłonny i wymaga zaangażowania specjalistów, co również wpływa na ostateczne koszty.

Jednak pomimo wyższych kosztów początkowych, uzyskanie certyfikatów ekologicznych może przynieść wymierne korzyści w dłuższym okresie. Zwiększona efektywność energetyczna, niższe koszty operacyjne, a także poprawa wizerunku firmy jako lidera zrównoważonego rozwoju mogą przekładać się na większą konkurencyjność na rynku oraz przyciąganie klientów, dla których kwestie ekologiczne są ustalonym priorytetem.



Regulacje dotyczące emisji CO_2 oraz rosnące znaczenie certyfikatów ekologicznych stanowią istotne wyzwania dla operatorów centrów danych. Wdrażanie strategii zwiększających efektywność energetyczną, integracja odnawialnych źródeł energii oraz dążenie do uzyskania certyfikatów takich jak LEED, BREEAM czy Green Globes to nie tylko krok w kierunku wykazania spełnienia wymogów narzucanych przez ustawodawców (tak krajowych jak i unijnych) lub doraźnego obniżenia kosztów prowadzenia działalności, ale również strategia zrównoważonego rozwoju, która może przynieść długoterminowe korzyści. W obliczu globalnych wyzwań związanych z klimatem, te działania stają się nieodzownym elementem odpowiedzialnego zarządzania nowoczesnymi centrami danych.

[1]https://climate.ec.europa.eu/eu-action/eu-emissions-trading-system-eu-ets/ets2-buildings-road-transport-and-additional-sectors_en?prefLang=pl&etrans=pl
[2]https://www.iea.org/energy-system/buildings/data-centres-and-data-transmission-networks

2. GO LOCAL / RELOKALIZACJA

PRZEPISY DOTYCZĄCE LOKALIZACJI DANYCH

Jakub Kulesza
Forum Prawo do Rozwoju

Lokowanie danych: Niektóre jurysdykcje wymagają, aby dane osobowe były przechowywane na serwerach zlokalizowanych w kraju, w którym dane zostały zebrane. Może to wymagać od operatorów centrów danych inwestycji w lokalne centra danych.

Wprowadzenie

Przepisy dotyczące lokalizacji danych są coraz bardziej istotnym elementem regulacji prawnych na całym świecie, w tym w Europie. Wymagają one, aby dane osobowe były przechowywane i przetwarzane na serwerach zlokalizowanych w kraju, w którym dane te zostały zebrane[1]. Takie regulacje mają na celu ochronę suwerenności danych oraz zabezpieczenie ich przed dostępem nieautoryzowanych podmiotów z zagranicy[2]. Jednak przepisy te mogą prowadzić do poważnych wyzwań operacyjnych i finansowych dla firm działających w sektorze centrów danych, które muszą dostosować się do różnych wymogów prawnych w zależności od jurysdykcji[3].

Lokowanie danych w Europie

W Europie podstawowe ramy regulacyjne w zakresie ochrony danych osobowych ustanawia Rozporządzenie Ogólne o Ochronie Danych Osobowych (RODO), które, choć bezpośrednio nie wymaga lokalizacji danych, wprowadza surowe ograniczenia dotyczące transferu danych osobowych poza Europejski Obszar Gospodarczy (EOG)[1]. W efekcie wiele krajów i organizacji europejskich wprowadza dodatkowe przepisy lub wytyczne, które w praktyce wymagają przechowywania danych na terenie Unii Europejskiej[2]. Przykładem są przepisy wprowadzone przez Niemcy i Francję, które obligują do lokalizowania pewnych kategorii danych, takich jak dane finansowe i zdrowotne, wyłącznie na ich terytorium[4].

Po decyzji Trybunału Sprawiedliwości Unii Europejskiej w sprawie Schrems II, która unieważniła mechanizm Privacy Shield, przepływ danych między UE a USA stał się jeszcze bardziej skomplikowany. Wiele firm operujących na rynku europejskim zaczęło inwestować w lokalne centra danych, aby uniknąć potencjalnych konfliktów prawnych wynikających z przetwarzania danych poza granicami UE[2].

Przepisy lokalizacyjne poza Europą

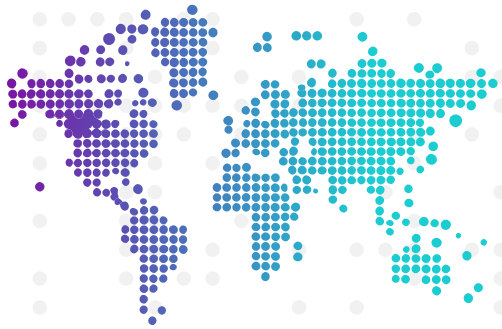
Podobne regulacje istnieją także w innych częściach świata. Na przykład **Rosja** od 2015 roku wymaga, aby dane osobowe rosyjskich obywateli były przechowywane na serwerach zlokalizowanych w Rosji. Ustawa ta jest jednym z najbardziej restrykcyjnych przykładów lokalizacji danych i obejmuje zarówno firmy lokalne, jak i zagraniczne, które prowadzą działalność w Rosji lub oferują usługi Rosjanom[5].

Chiny również wprowadziły surowe przepisy dotyczące lokalizacji danych, które wymagają, aby różne formy danych, w tym dane osobowe i "dane ważne", były przechowywane lokalnie i poddawane rządowej kontroli przed ich transferem za granicę. Podobne regulacje mają na celu zwiększenie kontroli nad cyfrową infrastrukturą oraz ograniczenie dostępu do danych przez zagraniczne podmioty[3].

Wyzwania operacyjne i implikacje dla rynku data center

Przepisy dotyczące lokalizacji danych stwarzają znaczące wyzwania dla firm działających na rynku centrów danych. Z jednej strony, zmuszają one firmy do inwestowania w lokalne infrastruktury IT, co może prowadzić do zwiększenia kosztów operacyjnych[3]. Z drugiej strony, takie regulacje fragmentaryzują globalny rynek danych, utrudniając swobodny przepływ informacji między różnymi krajami[6]. Firmy muszą dostosować swoje strategie zarządzania danymi do wymogów prawnych obowiązujących w różnych jurysdykcjach, co często oznacza konieczność utrzymywania serwerów i infrastruktury w wielu krajach[7].

Jednocześnie, rosnące wymagania dotyczące lokalizacji danych mogą zwiększać bezpieczeństwo przetwarzanych informacji, ponieważ dane są chronione przed dostępem podmiotów z krajów o mniej rygorystycznych przepisach ochrony danych[3]. Jednakże, dla globalnych korporacji technologicznych, takie regulacje mogą stanowić istotne ograniczenie w dostępie do globalnych rynków i wymuszać złożone decyzje dotyczące lokalizacji centrów danych[6].



Przyszłość przepisów dotyczących lokalizacji danych

W związku z dynamicznie zmieniającym się krajobrazem regulacyjnym, operatorzy centrów danych muszą być przygotowani na dalsze zaostrzanie przepisów dotyczących lokalizacji danych[7].

W przyszłości możliwe jest, że coraz więcej krajów będzie wprowadzać surowe wymagania lokalizacyjne, aby chronić swoją cyfrową suwerenność[6].

W takim kontekście firmy będą musiały nadal inwestować w lokalne centra danych, jednocześnie poszukując rozwiązań technologicznych, które pozwolą na zachowanie zgodności z przepisami bez nadmiernego zwiększania kosztów operacyjnych[7].

Podsumowując, przepisy dotyczące lokalizacji danych są kluczowym elementem zarządzania ryzykiem i zgodnością w globalnym środowisku cyfrowym. Wymagają one od operatorów centrów danych elastyczności, innowacyjności oraz gotowości do inwestowania w infrastrukturę, która spełnia wymogi prawne różnych jurysdykcji, zapewniając jednocześnie bezpieczeństwo i dostępność danych[6].

[1]European Union, GDPR - General Data Protection Regulation. Official Journal of the European Union., dostęp 29.08.2024 r.: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[2]Schrems II Judgment. Court of Justice of the European Union, 07.2020, dostęp 29.08.2024 r.: https://curia.europa.eu/juris/document/document.jsf?docid=228677&text=&dir=&doclang=EN&part=1&occ=first&mode=DOC&pageIndex=0&cid=104255

[3]The Real National Security Concerns over Data Localization. Center for Strategic and International Studies (CSIS), 2021, dostęp 29.08.2024 r.: https://www.csis.org/analysis/real-national-security-concerns-over-data-localization

[4]Health data hosting: The new French HDS Certification has been released. Hogan Lovells, 05.2024 r., dostęp 29.08.2024 r.: https://www.engage.hoganlovells.com/knowledgeservices/news/health-data-hosting-the-new-french-hds-certification-has-been-released

[5]Russia's Federal Law No. 242-FZ on Personal Data. Roskomnadzor, dostęp 29.08.2024 r.: https://pd.rkn.gov.ru/authority/p146/p191/

[6]Data Residency Laws by Country: an Overview. In Country, 2021 r., dostęp: 29.08.2024 r.: https://incountry.com/blog/data-residency-laws-by-country-overview/amp/

[7] Is Data Localization Coming to Europe?, IAPP (International Association of Privacy Professionals), 08.2022 r., dostęp 29.08.2024 r.: https://iapp.org/news/a/is-data-localization-coming-to-europe

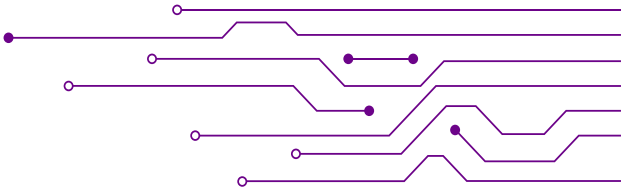
3. NIS ERA / ERA NIS
REGULACJE DOTYCZĄCE USŁUG W CHMURZE

Kamil Klepacki
Kierownik zespołu prawnego w COI

Marta Cudziło
Radca prawny w COI

Bezpieczeństwo i zgodność usług chmurowych: Operatorzy centrów danych oferujących usługi chmurowe muszą zapewniać zgodność z przepisami dotyczącymi bezpieczeństwa, prywatności i ochrony danych, zarówno na poziomie krajowym, jak i międzynarodowym.

Wiele podmiotów wciąż staje przed dylematem, czy aby zapewnić optymalne funkcjonowanie prowadzonej działalności wybrać usługę chmurową, czy może postawić na opcję infrastruktury lokalnej. Jeżeli chodzi o rozwiązania chmurowe to główną ich ideą jest inwestycja w moc obliczeniową, zamiast jak odbywało się to do tej pory – w sprzęt komputerowy. Rozwiązania chmurowe stają się więc coraz bardziej popularne jednak przed operatorami centrów danych oferujących usługi chmurowe stoi wiele wyzwań i wymagań, w szczególności w takich obszarach jak zapewnienie zgodności z przepisami prawa powszechnie obowiązującego dotyczącymi bezpieczeństwa, prywatności oraz ochrony danych, zarówno na poziomie krajowym, jak i międzynarodowym. Jest to o tyle istotne, że możliwości jakie oferują nowoczesne technologie cyfrowe są także wykorzystywane w celu stosowania praktyk nieuczciwej konkurencji, przerywania ciągłości działania wybranych usług, popełniania przestępstw z wykorzystaniem Internetu, czy też prowadzenia działań o charakterze terrorystycznym[1]. Usługi chmury obliczeniowej nie zostały jednak uregulowane w jednym akcie prawnym, co może utrudniać zapewnienie zgodności z ww. przepisami[2].



Omówienie jednak wszystkich regulacji w tym zakresie wykracza poza ramy przedmiotowego artykułu. Dlatego skupimy się w nim przede wszystkim na przepisach z zakresu ochrony danych osobowych oraz krajowego systemu cyberbezpieczeństwa, sygnalizując jednak również inne kwestie.

W pierwszej kolejności należy wskazać na Dyrektywę NIS, dotyczącą bezpieczeństwa sieci i informacji[3]. Należy także wymienić Dyrektywę NIS 2, która wprowadza nowe wymagania dotyczące bezpieczeństwa sieci i systemów informatycznych w UE, na której wdrożenie państwa członkowskie mają czas do 17 października 2024 r.[4]

Dyrektywa NIS zobowiązała wszystkie państwa członkowskie UE do zagwarantowania minimalnego poziomu zdolności krajowych w dziedzinie cyberbezpieczeństwa przez ustanowienie organów właściwych oraz pojedynczego punktu kontaktowego do spraw cyberbezpieczeństwa, powołanie zespołów reagowania na incydenty komputerowe (CSIRT) oraz przyjęcia krajowych strategii w zakresie cyberbezpieczeństwa.

Powyższa dyrektywa została wdrożona do polskiego porządku prawnego na mocy ustawy z dnia 5 lipca 2018 r. o Krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077), (dalej jako **„ustawa o KSC”**).

Celem Krajowego systemu cyberbezpieczeństwa jest zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów.

Krajowy system cyberbezpieczeństwa obejmuje szereg podmiotów, których można podzielić na operatorów usług kluczowych, dostawców usług cyfrowych oraz na podmioty publiczne. Z punktu widzenia zakresu niniejszego artykułu kluczowe znaczenie należy nadać dostawcom usług cyfrowych. Zanim przejdziemy do opisania dostawców usług cyfrowych należy zaznaczyć, że przez usługę przetwarzania w chmurze rozumie się taką usługę cyfrową, która umożliwia dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania przez wielu użytkowników[5].

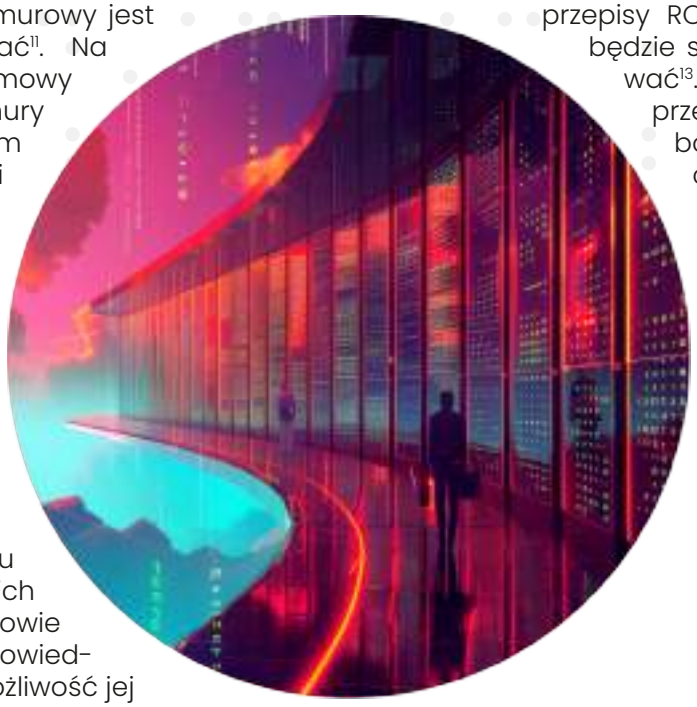
Dostawcą usługi cyfrowej jest osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej mająca siedzibę lub zarząd na terytorium Rzeczypospolitej Polskiej albo przedstawiciela mającego jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, świadcząca usługę cyfrową, z wyjątkiem mikroprzedsiębiorców i małych przedsiębiorców. Istotnym jest także wskazanie, że dostawca usługi cyfrowej jest zobowiązany do podejmowania właściwych i proporcjonalnych środków technicznych i organizacyjnych określonych w rozporządzeniu wykonawczym 2018/151[6] w celu zarządzania ryzykiem, na jakie narażone są systemy informacyjne wykorzystywane do świadczenia usługi cyfrowej. Środki te zapewniają cyberbezpieczeństwo odpowiednie do istniejącego ryzyka oraz uwzględniają bezpieczeństwo systemów informacyjnych i obiektów, postępowanie w przypadku obsługi incydentu, zarządzanie ciągłością działania dostawcy w celu świadczenia usługi cyfrowej, monitorowanie, audyt i testowanie, najnowszy stan wiedzy, w tym zgodność z normami międzynarodowymi, o których mowa w ww. rozporządzeniu wykonawczym 2018/151[7].

Dostawcy usług cyfrowych muszą więc zapewnić odpowiednie środki bezpieczeństwa systemów informacyjnych. Zgodzić się należy z tymi autorami, którzy **przez bezpieczeństwo systemów informacyjnych uznają taki poziom uzasadnionego zaufania, że ewentualne straty wynikające z przypadkowego, czy też świadomego ujawnienia, modyfikacji, zniszczenia lub uniemożliwienia przetwarzania informacji przechowywanej i przesyłanej za pomocą systemów teleinformatycznych, nie zostaną poniesione[8].** Bezpieczeństwo teleinformatyczne musi być rozpatrywane na płaszczyźnie organizacyjnej, technicznej czy też prawnej. Bezpieczeństwo jest więc ciągłym, dynamicznym oraz złożonym procesem, który wymaga stałego nadzoru i przystosowywania się do zmiennych warunków wewnętrznych oraz zewnętrznych[9].

Nawiązując do wskazanej już wyżej Dyrektywy NIS 2 należy zaznaczyć, że zakłada ona m.in. podział sektorów gospodarki oraz wskazuje na podmioty kluczowe oraz podmioty ważne objęte jej zakresem. Do sektorów kluczowych zalicza ona również infrastrukturę cyfrową, która swoim pojęciem obejmuje m.in. dostawców usług chmurowych, natomiast samą usługę chmurową określa jako usługę cyfrową umożliwiającą administrowanie na żądanie skalowalnym i elastycznym zbiorem zasobów obliczeniowych do wspólnego wykorzystywania oraz szeroki dostęp zdalny do tego zbioru, w tym również gdy takie zasoby są rozproszone w kilku lokalizacjach. Wskutek powyższego,

na mocy Dyrektywy NIS 2, dostawcy usług chmurowych działający w sektorze kluczowym i niebędący małym/mikro/średnim przedsiębiorcą będą stanowić podmiot kluczowy zobowiązany do wdrożenia odpowiednich i proporcjonalnych środków technicznych, operacyjnych i organizacyjnych[10].

Przedstawiona analiza prowadzi więc do wniosku, że na operatorach usług chmurowych spoczywa wiele obowiązków aby możliwym było zapewnienie odpowiedniego bezpieczeństwa tj. określonego przepisami prawa powszechnie obowiązującego. Z drugiej zaś strony, należy pamiętać, że również osoby (podmioty), które będą decydowały się na konkretnego dostawcę usługi chmurowej powinny dokonać analizy ryzyka już na etapie wyboru takiego dostawcy. Taka weryfikacja, pod kątem przepisów RODO może nastąpić na podstawie np. ankiety bezpieczeństwa, której operator usług chmurowy jest zobowiązany się poddać[11]. Na etapie podpisania umowy o świadczenie usług chmury obliczeniowej z danym dostawcą należy z kolei pamiętać, o wprowadzeniu (w miarę możliwości) odpowiednich postanowień odnośnie zapewnienia przez dostawcę wymagań w zakresie bezpieczeństwa, o których będzie mowa przy okazji analizy umowy powierzenia przetwarzania danych osobowych. W przypadku braku spełniania takich wymogów, w ww. umowie powinny znaleźć się odpowiednie kary umowne oraz możliwość jej wypowiedzenia. Aby jednak było możliwym sprawdzenie, czy określone warunki bezpieczeństwa zostały spełnione, w umowie o świadczenie usług chmury obliczeniowej powinna znaleźć się możliwość przeprowadzenia kontroli w tym zakresie.



W kontekście danych, zarówno osobowych jak i nieosobowych, operatorzy oferujący usługi chmurowe są zobowiązani do podjęcia wielu działań aby zachować zgodność z przepisami prawa w tym zakresie, w szczególności z RODO. Jeżeli chodzi o obszar danych osobowych, to w relacji operator chmury, a klient korzystający z usług takiego podmiotu, operator występuje w roli podmiotu przetwarzającego dane osobowe, które powierza mu do przetwarzania administrator danych czyli klient. Zatem, należy wskazać, że to klient podejmuje decyzję o celach przetwarzania danych osobowych i jego zakresie, podczas gdy operator chmurowy decyduje o kwestiach technicznych rozwiązania chmurowego. Dla przyjęcia zastosowania RODO nie ma znaczenia, gdzie odbywa się przetwarzanie danych osobowych – istotne jest wyłącznie to, czy przetwarzanie odbywa się w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w UE[12].

Jeżeli jednak przetwarzanie danych osobowych odbywa się w miejscu, w którym na mocy prawa międzynarodowego publicznego ma zastosowanie prawo państwa członkowskiego UE, wówczas zastosowanie będą miały przepisy RODO, a operator chmury będzie się musiał do nich stosować[13]. W związku z powyższym, przetwarzanie danych osobowych przez operatora chmury nastąpi na podstawie umowy powierzenia przetwarzania danych osobowych, do której zawarcia zobowiązany jest procesor i administrator danych[14].

Dostawca usług chmurowych będzie również zobowiązany do prowadzenia rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora (klienta)[15]

W kontekście bezpieczeństwa należy także pamiętać, że w przypadku nie dopełnienia przez podmiot przetwarzający obowiązków wynikających z RODO, podmiot taki odpowiada za szkodę w tym zakresie[16].

W przypadku gdy korzystanie z usług chmurowych będzie wiązało się z przekazaniem danych osobowych do państwa trzeciego poza EOG przez administratora danych podlegającego RODO z uwagi na zlokalizowanie dostawcy chmurowego poza EOG, dostawca usługi chmurowej musi również spełnić szereg obowiązków aby móc je przetwarzać. W związku z koniecznością transferu, na podstawie RODO możemy wyróżnić trzy współzależne i hierarchicznie uporządkowane mechanizmy legalizacji transferów danych osobowych: decyzja KE, która stwierdza odpowiedniość ochrony w państwie trzecim, odpowiednie zabezpieczenia ochrony danych osobowych jeżeli nie została wydana taka decyzja jak np.: wiążące reguły korporacyjne czy standardowe klauzule ochrony danych oraz pozostałe mechanizmy, jeżeli dwa wcześniejsze nie mają zastosowania[17].

Powyższe rozważania dotyczą przepisów prawa w zakresie danych osobowych - a co z regulacjami prawnymi w zakresie danych nieosobowych? W tej materii obowiązują przepisy, które przewidują możliwość tworzenia samoregulacyjnych unijnych kodeksów postępowania regulujących m.in. ułatwienia w zakresie zmiany dostawcy usług i przenoszenia danych do innych dostawców[18]. Należy również wspomnieć o przepisach, które wpłyną na dostawców usług chmurowych poprzez tak zwany „Data Act"[19].

Zgodnie z art. 23 Data Act dostawcy usług przetwarzania danych będą zobowiązani do stosowania środków, które umożliwią ich klientom zmianę usługi przetwarzania danych na usługę tego samego typu świadczoną przez innego dostawcę, lokalną infrastrukturę ITC lub korzystanie z usług kilku dostawców.

Ostatnią kwestią, którą należy zasygnalizować jest zapewnienie przez operatorów centrów danych oferujących usługi chmurowe zgodności z przepisami prawa dotyczącymi ochrony prywatności. Pod tym kątem należy wskazać na przepisy RODO, w którym wyszczególniono m.in. uprawnienia polegające na możliwości żądania od administratora danych dostępu do danych osobowych, ich sprostowania, usunięcia (prawo do bycia zapomnianym), przenoszenia lub ograniczenia przetwarzania, wniesienia sprzeciwu wobec przetwarzania danych oraz skargi do organu nadzorczego.

Powyższa analiza w zakresie zapewnienia przez operatorów oferujących usługi chmurowe zgodności z regulacjami prawnymi dotyczącymi bezpieczeństwa, prywatności i ochrony danych zarówno na poziomie krajowym jak i międzynarodowym prowadzi do wniosku, że regulacje prawne w tym zakresie mają charakter rozproszony. W związku z powyższym, niezwykle istotnym jest zidentyfikowanie wszystkich źródeł prawa, które będą miały zastosowanie do dostawców usług chmurowych aby w obliczu transformacji cyfrowej i rozwijającej się niezwykle dynamicznie technologii chmurowej w segmencie IaaS, PaaS czy SaaS, operatorzy chmurowi byli zgodni z obowiązującymi regulacjami prawnymi. Powyższe, będzie gwarancją, że oferowane przez operatorów usługi chmurowe będą bezpieczne, a tym samym chroniące prywatność osób fizycznych i przetwarzane w nich dane.

[1] Uzasadnienie projektu ustawy z dnia 30 kwietnia 2018 r. o Krajowym systemie cyberbezpieczeństwa, VIII.2505 (dostęp LEX, 22.08.2024 r.).
[2] Przepisy w tym zakresie możemy znaleźć w przepisach o ochronie danych osobowych, przepisach o krajowym systemie cyberbezpieczeństwa, przepisach sektorowych (np. usługi finansowe), w przepisach dotyczących praw własności intelektualnej (prawo autorskie, ochrona baz danych), czy też w przepisach prawa cywilnego (umowa o świadczenie usług chmury obliczeniowej).
[3] 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. U. UE. L. z 2016 r. Nr 194, str. 1). Dyrektywa ta traci moc ze skutkiem od dnia 18 października 2024 r. (na podstawie art. 44 dyrektywy wskazanej w przypisie nr 4).
[4] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (Dz.U. L 333 z 27.12.2022). Na dzień 29 sierpnia 2024 r. dyrektywa ta nie została implementowana do polskiego porządku prawnego. Implementację ww. dyrektywy przewiduje projekt ustawy z dnia 24 kwietnia 2024 r. o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw https://legislacja.rcl.gov.pl/projekt/12384504 (dostęp dnia 27.08.2024).
[5] Definicja zawarta w załączniku nr 2 do ustawy o KSC.
[6] Rozporządzenie wykonawcze Komisji (UE) 2018/151 z dnia 30 stycznia 2018 r. ustanawiające zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ (Dz. U. UE. L. z 2018 r. Nr 26, str. 48).
[7] Zob. art. 17-18 ustawy o KSC.
[8] W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz (red.), Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz do art. 8, Warszawa 2019 (dostęp Legalis 26.08.2024 r.).
[9] Ibidem.
[10] Wynika to z art. 21 ust. 2 Dyrektywy NIS 2, który określa minimalny katalog środków jakie musi zapewnić podmiot kluczowy, wśród których jest m.in.: polityka analizy ryzyka i bezpieczeństwa systemów informatycznych, obsługa incydentu, ciągłość działania czy bezpieczeństwo łańcucha dostaw.
[11] Art. 28 Rozporządzenia 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 (ogólne rozporządzenie o ochronie danych) z dnia 27 kwietnia 2016 r. (Dz. Urz. UE. L Nr 119, poz. 1), (dalej jako „RODO").
[12] Por. art. 3 ust. 1 RODO.
[13] Komentarz do art. 3 RODO [w:] P. Litwiński (red.), Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz, 2021 (dostęp Legalis 26.08.2024 r.).
[14] Wynika to z art. 28 ust. 3 RODO, który określa minimalny katalog zobowiązań jakie musi spełnić podmiot przetwarzający na podstawie takiej umowy powierzenia przetwarzania danych osobowych. Przepis ten wskazuje m.in. że podmiot przetwarzający może przetwarzać dane osobowe wyłącznie na udokumentowane polecenie administratora danych, musi wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku czy też zapewnić, aby osoby upoważnione do przetwarzania danych osobowych były zobowiązane do zachowania tajemnicy.
[15] Por. art. 30 ust. 2 RODO.
[16] Zob. art. 82 RODO.
[17] Zob. w tym zakresie art. 45-47 RODO oraz komentarz do art. 44 RODO [w:] P. Litwiński (red.), Ogólne rozporządzenie (...) op. cit. (dostęp Legalis, 26.08.2024 r.).
[18] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej (Dz. U. UE. L. z 2018 r. Nr 303, str. 59).
[19] Chodzi o Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/2854 z dnia 13 grudnia 2023 r. w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania oraz w sprawie zmiany rozporządzenia (UE) 2017/2394 i dyrektywy (UE) 2020/1828 (akt w sprawie danych) (Dz. U. UE. L. z 2023 r. poz. 2854). (dalej: „Data Act"), które stosuje się od 12 września 2025 r.

4. DATA CENTER REIT / REIT CENTRÓW DANYCH

STAN ZAAWANSOWANIA PRAC LEGISLACYJNYCH NAD REIT (REAL ESTATE INVESTMENT TRUST) W POLSCE

Konrad Hennig
Forum Prawo dla Rozwoju

REIT (ang. Real Estate Investment Trust) to objęte preferencjami podatkowymi fundusze inwestycyjne lub spółki notowane na giełdzie, lokujące aktywa indywidualnych inwestorów w nieruchomości komercyjne. Ich formuła wywodzi się ze Stanów Zjednoczonych i tam też najwięcej jest inwestycji funduszy REIT w centra danych. Spełniają one podstawowe kryterium przewidywalności biznesu w oparciu o dywersyfikację portfela najemców, podobnie jak galerie handlowe czy biurowce. W USA działa kilkadziesiąt funduszy skoncentrowanych na centrach danych, dysponujących około 10% powierzonych środków. Inwestują nie tylko w USA, a największe REIT-y mają w portfolio nawet kilkaset centrów danych rozsianych po całym świecie.

Polska nie wdrożyła jak dotąd regulacji określających obowiązki i przywileje funduszy inwestujących w nieruchomości na wynajem ze względu na obawę zaburzenia cen na rynku mieszkaniowym.

Przyjęcie jednolitej regulacji prawnej dotyczącej REIT z wyłączeniem możliwości zakupu mieszkań na wynajem zapewniłoby dopływ dodatkowych środków do sektora nieruchomości komercyjnych oraz umożliwiłoby drobnym inwestorom alternatywę wobec zakupu mieszkań na wynajem, redukując presję cenową w największych miastach wojewódzkich.

Na skutek zaniedbań ustawodawcy, ale również wysokiej awersji do ryzyka Polaków, finansowanie przedsięwzięć rozwojowych jest w znacznej mierze zależne od kapitału zagranicznego i mało efektywnego finansowania publicznego.

Obecnie ustawa z dnia 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi dopuszcza aby polityka inwestycyjna funduszy inwestycyjnych zamkniętych aktywów niepublicznych (FIZAN) przewidywała inwestowanie w nieruchomości, niemniej jednak z uwagi na mocno sformalizowaną strukturę, wysokie koszty zarządzania, sposób opodatkowania oraz niską płynność przy wyjściu z inwestycji model inwestowania w nieruchomości przez FIZAN jest nieefektywny. Powyższe potwierdza również praktyka rynkowa, na przykładzie sankcji nałożonych na FinCrea TFI S.A. w związku z nieprawidłowym zarządzaniem funduszami nieruchomościowymi[1].

Jeśli chodzi natomiast o inwestowanie w nieruchomości za pośrednictwem alternatywnych spółek inwestycyjnych (ASI), KNF podkreśla jak istotną rolę odgrywa dywersyfikacja portfela inwestycyjnego w celu ochrony inwestorów oraz zgodność z unijną definicją alternatywnego funduszu inwestycyjnego, którego odmianą na polskim rynku jest ASI. Z tego względu **na rynku można zaobserwować trend, w którym KNF rejestruje jedynie tych zarządzających ASI, którzy nie deklarują w politykach inwestycyjnych ASI 100% bezpośredniego zaangażowania w nieruchomości.** Z tego względu inwestowanie w nieruchomości za pośrednictwem ASI odbywa się najczęściej przy wykorzystaniu spółek celowych lub inwestycji pośrednich w podmioty działające w branży deweloperskiej oraz adresowane jest przede wszystkim do klientów profesjonalnych.

Począwszy od 2021 r. toczyły się prace ministerialne nad adaptacją REIT do krajowego porządku prawnego, włącznie z powołaniem Międzyresortowego Zespołu do opracowania

regulacji dotyczących podmiotów inwestujących w najem nieruchomości. W nowym układzie rządowym wiodącą rolę od ministra właściwego ds. gospodarki przejął Minister Finansów.

W czerwcu 2024 r. Andrzej Domański podczas Forum Funduszy w Kazimierzu Dolnym zapowiedział rychłe wprowadzenie REIT-ów. Stworzenie jednolitych ram prawnych dla REIT pozwoliłoby uzupełnić brakującą lukę na rynku kapitałowym poprzez zbiorowe inwestowanie w nieruchomości, mające prorozwojowy, a nie konsumpcyjny charakter.

Bez wątpienia centra danych, jako umożliwiające transformację cyfrową przedsiębiorstw powinny stanowić ważny, jeśli nie główny cel inwestycyjny polskich REIT-ów.

[1]https://www.knf.gov.pl/komunikacja/komunikaty?articleId=72856&p_id=18, data publikacji: 09.03.2021 r.
autor: Konrad Hennig, Stowarzyszenie Prawo dla Rozwoju.

3. ANALIZA RYNKU DATA CENTER W POLSCE

3A. PRZEGLĄD HISTORYCZNEGO ROZWOJU RYNKU DATA CENTER W POLSCE

Rozwój centrów danych w Polsce jest ściśle związany z rozwojem technologii informacyjnych i telekomunikacyjnych. Początki tego procesu sięgają lat 90., kiedy to pojawiły się pierwsze potrzeby przechowywania i przetwarzania danych na większą skalę.

1. Lata 90: Początki

Za pierwsze polskie data center uważa się centrum obliczeniowe, które powstało w 1994 roku w Warszawie, na potrzeby operatora telekomunikacyjnego TPSA (Telekomunikacja Polska S.A., obecnie Orange Polska). Było to jedno z pierwszych profesjonalnych centrów danych w Polsce, choć jego funkcje były ograniczone głównie do obsługi wewnętrznych potrzeb operatora.
Wraz z liberalizacją rynku telekomunikacyjnego i wzrostem zapotrzebowania na usługi internetowe, rozwijała się także infrastruktura IT. W tym czasie powstawały pierwsze sieci szkieletowe oraz systemy do zarządzania danymi[1].

2. Lata 2000 - 2010: Intensyfikacja rozwoju

Początek XXI wieku to czas, kiedy w Polsce zaczęły pojawiać się centra danych tworzone przez międzynarodowe korporacje. Firmy takie jak Atman, T-Mobile, czy Polkomtel zaczęły budować własne centra, aby zaspokoić rosnące potrzeby związane z przechowywaniem danych, co podniosło standardy usług i wprowadziło nowe technologie.

Wzrost popularności usług w chmurze w Polsce zaczął się od około 2008 roku. Polskie firmy zaczęły inwestować w data center, aby móc oferować usługi w modelu SaaS, PaaS i IaaS.

3. Lata 2010 - 2020: Era nowoczesnych data center

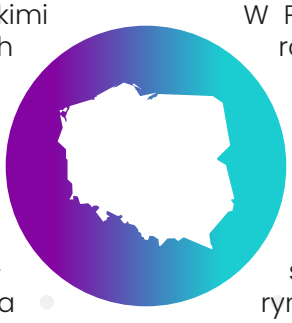
Na rynku pojawiło się wielu lokalnych dostawców usług data center, takich jak Beyond.pl, Netia Data Center czy ATM S.A. (obecnie Atman). Centra te oferowały już zaawansowane usługi, w tym outsourcing IT, kolokację, a także kompleksowe rozwiązania chmurowe.
Wraz z rozwojem rynku, coraz większy nacisk kładziono na bezpieczeństwo danych oraz zgodność z regulacjami prawnymi, takimi jak RODO. Nowoczesne centra danych w Polsce musiały spełniać najwyższe standardy w zakresie bezpieczeństwa fizycznego i cyfrowego.
Wzrost popularności usług chmurowych, takich jak AWS, Microsoft Azure czy Google Cloud, a w rezultacie budowa lokalnych zasobów chmurowych, wymusiła rozwój infrastruktury data center wspierającej te usługi.

3B. AKTUALNY STAN RYNKU DATA CENTER

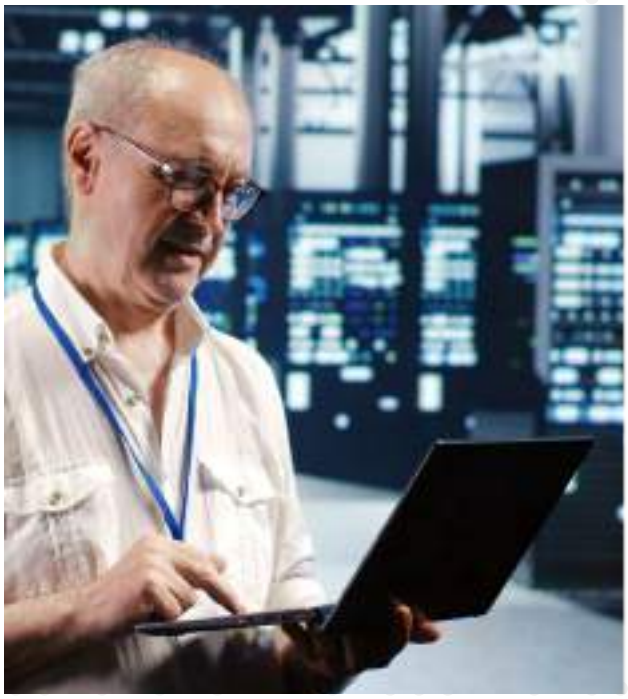
Rynek data center w Polsce dynamicznie się rozwija, odzwierciedlając globalne trendy w cyfryzacji, przetwarzaniu danych oraz wzroście zapotrzebowania na usługi chmurowe. Polska staje się jednym z kluczowych hubów data center w Europie Środkowo-Wschodniej dzięki strategicznemu położeniu, stabilnej infrastrukturze oraz rosnącej liczbie inwestycji zarówno krajowych, jak i zagranicznych firm[3] .

W ostatnich latach rośnie także znaczenie zrównoważonego rozwoju w obszarze data center. Polskie centra danych coraz częściej korzystają z odnawialnych źródeł energii oraz stosują technologie chłodzenia przyjazne środowisku.

Kołem zamachowym rozwoju sektora była pandemia Covid-19, która spowodowała przyspieszenie cyfrowej transformacji i rosnące zapotrzebowanie na usługi data center w związku z pracą zdalną i zwiększonym wykorzystaniem usług online.



W Polsce, podobnie jak na całym świecie, rozwijają się technologie związane z big data, AI oraz Internetem Rzeczy (IoT), co powoduje, że centra danych muszą sprostać jeszcze większym wymaganiom w zakresie skalowalności i wydajności, a także stale poprawiać rozwiązania technologiczne, aby sprostać szybko zmieniającym się wymogom na rynku.



[2]https://www.encyclopedia.com/books/politics-and-business-magazines/telekomunikacja-polska-sa
[3]Pisaliśmy o tym w raporcie pokonferencyjnym podsumowującym pierwszą edycję Forum Data Center z 2023 r.: "Budowanie przyszłości centrów danych".

Stan rynku data center w Polsce w 2024 roku

1. Liczba i lokalizacja centrów danych:

- W 2024 roku rynek data center w Polsce dynamicznie się rozwija, a liczba centrów danych osiągnęła 112 obiektów. Większość z tych ośrodków to mniejsze jednostki, ale 65 z nich ma powierzchnię powyżej 200 m². Rozwój ten jest napędzany przez rosnące zapotrzebowanie na usługi chmurowe, sztuczną inteligencję oraz cyfryzację biznesu.

65 DC ma powierzchnię powyżej 200m2

- Najwięcej centrów danych znajduje się w Warszawie, co jest strategicznym wyborem ze względu na dostępność infrastruktury oraz wykwalifikowanej kadry. Inne ważne lokalizacje to Kraków, Wrocław i Poznań, gdzie także funkcjonuje kilka większych centrów danych. W przyszłości spodziewane jest dalsze powstawanie nowych obiektów oraz konsolidacja rynku, co może prowadzić do zamykania mniejszych, mniej efektywnych jednostek.

GŁÓWNIE WARSZAWA

2. Nowoczesność i skalowalność:

- Coraz więcej centrów danych spełnia standardy Tier III i Tier IV, co zapewnia wysoką dostępność i niezawodność usług.

- Inwestycje w energooszczędne technologie i systemy chłodzenia, co jest odpowiedzią na rosnące wymagania ochrony środowiska.

3. Rynek pracy i rozwój kompetencji:

- Wzrost zapotrzebowania na specjalistów IT oraz inwestycje w rozwój kompetencji w obszarze zarządzania centrami danych.

3C. PERSPEKTYWA EUROPEJSKA I ŚWIATOWA

Adam Wnorowski
Prezes, Instytut Transformacji

Rynek centrów danych przeżywa obecnie niesamowity okres popytu. Po masowym wzroście zapotrzebowania na przestrzeń i moc w adopcji rozwiązań chmurowych, przyszedł czas na jeszcze większy hype: sztuczną inteligencję.

Dotychczasowe szafy rackowe obsługiwały średnio urządzenia z zapotrzebowaniem mocy w przedziale 3-7kW, obecne wymogi sięgają od 12 do nawet 130 kW, w zależności od zastosowanej technologii i metody chłodzenia.

Same zaś obiekty centrów danych - ze standardowych 4-10MW - muszą zmienić architekturę by sprostać zapotrzebowaniu na obiekty nie mniejsze niż kilkadziesiąt MW, a nawet do 1GW w przypadku megakampusów.

Rynek polski centrów danych jest określany jako Tier II, co oznacza, że aspiruje do grona rynków potencjalnego wzrostu i ma okazję stać się kuszącym kąskiem w oczach inwestorów. Nareszcie lokalizacja Polski może odegrać pozytywną rolę i skutecznie stać się zarówno dochodową branżą, spajającą ogromny potencjał intelektualny naszych rodaków w dziedzinie szeroko pojętej informatyki i robotyki, korzystać z ciągłego wzrostu przychodów i rosnącej gospodarki w postaci sektora informatycznego oraz energetycznego, jak również stać się jeszcze większym, bardziej znaczącym pomostem między zachodnią Europą a krajami po naszej wschodniej stronie (tym bardziej w obecnej sytuacji geopolitycznej).

W odniesieniu do skali globalnej, rynek data center w Polsce jest stosunkowo mały. Mówimy obecnie o około 200 MW mocy w centrach danych z początkiem 2025 roku oraz projekcjami wskazującymi na około 500 MW do roku 2030. Dla porównania, światowy rynek szacowany jest na około 45 tysięcy MW mocy IT (z czego ok. 12 tys. MW w Europie). Daje to Polsce niespełna 1% udziału w rynku.

Obecnie rozwojowi tego segmentu gospodarki sprzyjają nam warunki wprowadzonego w części Amsterdamu moratorium na budowę nowych obiektów oraz brak możliwości budowy centrów danych w Dublinie (brak mocy). Zapotrzebowanie na energię jest kluczowe, a jej brak odczuwalny nie tylko w Europie. Dlatego też, aby wykorzystać obecny czas w możliwie najlepszy sposób, potrzebne są zmiany w strategii i koncentracja działań na szczeblu rządowym oraz inwestorskim. Tu z pomocą przychodzi Instytut Transformacji, którego celem jest wspieranie sektora centrów danych oraz gałęzi przemysłu energochłonnego przy jednoczesnym wsparciu rządu w transformacji energetycznej kraju w kierunku alternatywnych źródeł

energii i modelu jej dystrybucji.

Przy optymalnym wykorzystaniu posiadanych zasobów, tempa rozwoju gospodarki i odpowiedniej koordynacji legislacyjno-projektowej, Polska ma szansę uzyskać znaczącą pozycję na arenie europejskiej. Transformacja cyfrowa - rozumiana jako zmiana podejścia do danych i usług cyfrowych - to potężne narzędzie nie tylko przychodów i dobrostanu społeczeństwa, ale także gwarant awansu do ligi krajów mocno ucyfrowionych i zaawansowanych technologicznie. W naszych czasach dane są złotem.

Aby to mogło się wydarzyć i abyśmy przyciągnęli więcej inwestorów, potrzebujemy konkurencji na polu kosztów energii, które potrafią stanowić nawet 70% kosztów projektu / usługi. Obecna sytuacja pozyskiwania energii głównie z węgla (około 42% energii produkujemy z węgla), przy jednoczesnym sporym koszcie certyfikatów emisji CO_2 nie pozwala nam konkurować z innymi krajami.

Należy nadać priorytet pracom, mającym na celu promowanie i umożliwienie pozyskiwania energii z alternatywnych źródeł: wodoru, atomu oraz biopaliw na szeroką skalę. W przeciwieństwie do fotowoltaiki czy farm wiatrowych, w centrach danych potrzeba stałych źródeł energii o relatywnie równym poborze energii w ciągu roku. W przypadku reaktorów nuklearnych Polska nie występuje w statystykach. W samej Europie w roku 2023 mieliśmy 167 reaktorów o łącznej mocy ponad 147 MWe.

W Czechach, znacznie mniejszych od Polski, jest ich aż 6. Niemcy, po wstępnym wygaszeniu reaktorów, mają spory dylemat i chcą wrócić do atomu jak najszybciej. Nawet uznawane za najbardziej ekologiczne kraje skandynawskie posiadają ich aż 11.

Nuclear Power Reactors in Operation in Europe, 24th May 2023 (https://www.euronuclear.org/glossary/nuclear-power-plants-in-europe/)

W naszym położeniu warto też – w perspektywie długofalowej – rozważyć elektrownie wodne, których co prawda nie brakuje, ale ich udział w miksie spada wraz ze wzrostem zapotrzebowania na prąd.
Przed nami sporo pracy i wyzwań, ale cel sam w sobie jest zgodny: należy redukować źródła

emisji CO_2, rozbudować alternatywne źródła mocy oraz usprawnić sieć przesyłową. Warto także skupić się na rozproszeniu źródeł energii jak najbliżej obiektów energochłonnych co pozwoli na spokojne i wymagające czasu inwestycje w kosztowną infrastrukturę przesyłową. Mamy ogromny potencjał i czas na długofalowe spojrzenie od strony legislacji. Kierunek alternatywnej energii nie powinien być elementem rozgrywek każdorazowo po wyborach. Potrzebujemy długofalowego planu inwestycji z jasno określonymi, mierzalnymi celami rozłożonymi w czasie. To element strategii ponad podziałami i dla dobra ogółu społeczeństwa oraz gospodarki.

Źródła: https://www.mordorintelligence.com/industry-reports/europe-colocation-market-industry
https://www.pmrmarketexperts.com/wiadomosci/do-2030-roku-wielkosc-rynku-centrow-danych-w-polsce-moze-przekroczyc-500-mw/
https://www.iea.org/countries/poland?language=es
https://www.infrastructureinvestor.com/power-struggles-emerge-as-ai-fuels-data-centre-growth/

3D. PRZEPISY PRAWNE I REGULACJE DOTYCZĄCE CENTRÓW DANYCH

1. OCHRONA DANYCH OSOBOWYCH

Katarzyna Blachowicz
Radca prawny, counsel
DGTL Kibil Piecuch
i Wspólnicy

Norbert Karmowski
Radca prawny

Powstawanie nowych i rozbudowa już funkcjonujących centrów przetwarzania danych, w następstwie rosnącego zapotrzebowania na usługi cyfrowe, niesie za sobą wyzwania w zakresie ochrony danych osobowych, w tym w obszarze zapewnienia poufności oraz integralności danych.

Rosnące wyzwania dla centrów przetwarzania danych

Ogólne rozporządzenie o ochronie danych osobowych (RODO[1]) nakłada na operatorów centrów danych (jako przetwarzających dane osobowe) szereg obowiązków mających na celu zapewnienie adekwatnego do ryzyk poziomu bezpieczeństwa przetwarzanych danych, w tym - obowiązek zapewnienia ochrony przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą danych, ich zniszczeniem lub uszkodzeniem. Dodatkowo, zapewnienie bezpieczeństwa przetwarzania danych nabiera istotnego znaczenia w dobie zwiększonego zagrożenia cyberatakami na infrastrukturę i systemy przetwarzania.
Należy podkreślić, że jedną z podstawowych zasad dotyczących ochrony danych osobowych jest zasada poufności i integralności, stosownie do której dane osobowe powinny być przetwarzane w sposób zapewniający należyte bezpieczeństwo danych osobowych.

Środki techniczne oraz organizacyjne zapewniające bezpieczeństwo danych

Stosownie do obowiązujących przepisów prawa podmiot przetwarzający dane (w tym operator centrum przetwarzania danych) zobligowany jest do wdrożenia właściwych środków technicznych oraz organizacyjnych, które zapewnią odpowiedni stopień bezpieczeństwa danych. Przykładowo, do rzeczonych środków zalicza się m.in. systemy kontroli dostępu, systemy sygnalizacji włamania i napadu, systemy monitoringu wizyjnego, systemy monitoringu parametrów środowiskowych oraz stanu pracy urządzeń czy wydzielenie dedykowanych stref bezpieczeństwa, zasilanie energią za pośrednictwem dwóch redundantnych linii zewnętrznych oraz wielostrefowe systemy przeciwpożarowe oparte na gazie obojętnym.

Przy ocenie tego jakie środki należy wdrożyć, aby zapewnić właściwy stopień bezpieczeństwa uwzględnia się: stan wiedzy technicznej, koszt wdrożenia oraz charakter, zakres, kontekst i cele przetwarzania danych, jak również ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze. Dokonując wyboru środków zabezpieczenia można posiłkować się wskazówkami ujętymi w art. 32 RODO. Mianowicie, do możliwych do zastosowania środków technicznych i organizacyjnych zalicza się między innymi: pseudonimizację i szyfrowanie danych osobowych; zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania; zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego; regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Co istotne, jak zostało wskazane wyżej, RODO wymaga, aby w przypadku incydentu fizycznego lub technicznego zastosowane środki bezpieczeństwa zapewniały zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich. Oznacza to, że w razie jakiegokolwiek incydentu dotyczącego infrastruktury bądź systemów centrów przetwarzania danych operator takiego centrum powinien jak najszybciej przywrócić osobom uprawnionym możliwość dostępu do danych osobowych oraz dokonywania na nich operacji.

Ocena ryzyka i dostosowanie środków bezpieczeństwa

Celem weryfikacji czy zastosowane przez dany podmiot środki zapewniają odpowiedni stopień bezpieczeństwa należy wziąć pod uwagę ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z: a) przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub b) nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Na uwagę zwraca fakt, że ogólna dyrektywa przyświecająca RODO – know your risk - nakłada na dysponentów danych obowiązek samodzielnej oceny ryzyk i stosowania adekwatnych mechanizmów im przeciwdziałających. W efekcie nie istnieje jeden "złoty standard" bezpieczeństwa centrum danych w kontekście RODO. Inne mechanizmy będą miały zastosowanie dla podmiotów przetwarzających dane instytucji finansowych, podlegających nadzorowi KNF/EBA (niezależnie od konieczności zapewnienia zgodności z regulacjami sektorowymi, takimi jak DORA), czy dla data center obsługujących podmioty przetwarzające dane szczególnie wrażliwe (np. jednostki z sektora usług ochrony zdrowia) - inne zaś ryzyko (a co za tym idzie: mniej restrykcyjne wymagania) mogą być zidentyfikowane dla data center obsługującego powszechnie dostępne serwisy informacyjne.

Niezastosowanie się do wymogów RODO w przedmiocie bezpieczeństwa przetwarzania danych może skutkować nałożeniem na dany podmiot kary pieniężnej, która w przypadku przedsiębiorstwa może wynieść do 2% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego.

Obowiązki operatorów centrów przetwarzania danych przy naruszeniu ochrony danych

W przypadku naruszenia ochrony danych osobowych, a więc przypadkowego lub niezgo-

dnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych, operator centrum przetwarzania danych (działając jako podmiot przetwarzający) jest zobowiązany każdorazowo po stwierdzeniu naruszenia ochrony danych osobowych dokonać stosownego zgłoszenia administratorowi danych osobowych. W literaturze przyjmuje się, że podmiot przetwarzający powinien zawiadomić administratora o każdym naruszeniu bez względu na to czy dane naruszenie może skutkować ryzykiem naruszenia praw lub wolności osób fizycznych. Ponadto wskazać należy, że przepisy RODO nie precyzują maksymalnego terminu w jakim takie zgłoszenie powinno być przekazane do administratora (RODO posługuje się w tym zakresie nieostrym zwrotem "bez zbędnej zwłoki").

Niemniej warto mieć na uwadze, że **niewypełnienie obowiązku przez procesora w zakresie zgłoszenia administratorowi naruszenia ochrony danych osobowych może skutkować nałożeniem kary pieniężnej bezpośrednio na administratora, który o dokonanym naruszeniu powinien powiadomić organ nadzoru maksymalnie w terminie 72 godzin.** Oznacza to, że niezgłoszenie administratorowi przez operatora data center incydentu fizycznego skutkującego naruszeniem ochrony danych osobowych może skutkować nałożeniem na klienta korzystającego z usług danego centrum danych kary pieniężnej w wysokości do 2% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego.

Podsumowanie i perspektywy dla centrów przetwarzania danych w zakresie ochrony danych

Mając na uwadze postęp technologiczny oraz transformację cyfrową, która dzieje się na naszych oczach, należy przypuszczać, że centra przetwarzania danych w dalszym ciągu w najbliższych latach będą się rozwijać, a co za tym idzie warto pamiętać, **że każdy podmiot przetwarzający dane jest zobligowany do systematycznej i cyklicznej weryfikacji czy zastosowane przez niego środki techniczne oraz organizacyjne odpowiadają ryzyku i zapewniają odpowiedni stopień bezpieczeństwa.** Raz wprowadzone środki zabezpieczenia nie zwalniają z odpowiedzialności za ewentualne szkody wynikające z naruszenia danych osobowych, a te mogą być znaczące w przypadku data center. Jako **dobre praktyki przyjąć należy przeprowadzanie regularnych audytów bezpieczeństwa, regularne szkolenia pracowników z zakresu ochrony danych osobowych czy też wdrażanie i aktualizowanie polityk bezpieczeństwa, najlepiej potwierdzonych odpowiednimi certyfikatami (np. z grupy ISO).** Operatorzy data center odgrywają istotną rolę w zapewnieniu bezpieczeństwa danych osobowych, w konsekwencji czego wdrożone przez nich środki bezpieczeństwa wymagają regularnego testowania i oceny oraz ciągłego monitorowania i dostosowywania procedur.

[1] Dz.Urz. UE.L Nr 119, poz. 1

2. BEZPIECZEŃSTWO INFORMACJI

Krzysztof Szczygieł

Prezes, Polski Instytut Data Center

Seria norm EN 50600 i jej znaczenie w branży centrów przetwarzania danych.

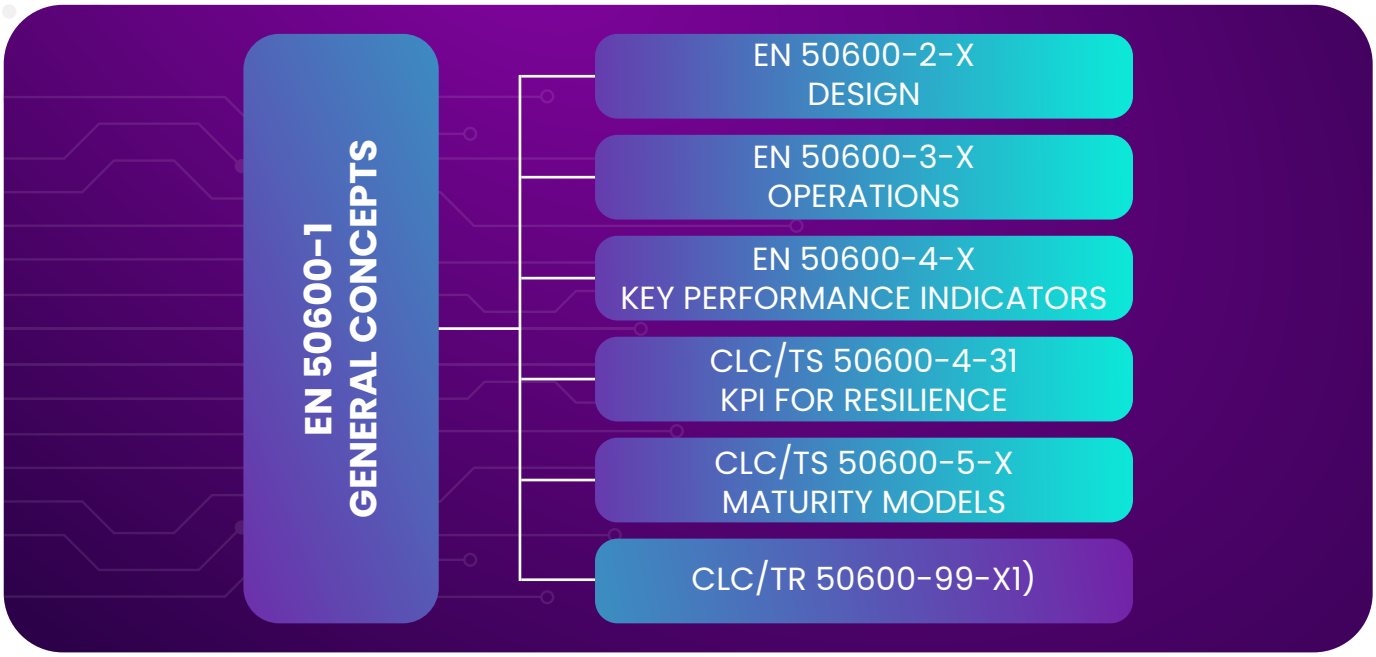
W ostatnich latach nastąpił duży zwrot w podejściu do normalizacji w branży centrów przetwarzania danych. Dynamicznie wzrasta zainteresowanie serią norm EN 50600 oraz ISO/IEC 22237.

Pierwsza norma z serii EN 50600, EN 50600-1 „Information technology - Data centre facilities and infrastructures - Part 1: General concepts" została wydana już w 2012 roku (EN 50600--1:2012, PN-EN 50600-1:2013), a prace normalizacyjne rozpoczęły się mniej więcej 3 lata wcześniej. Jednakże, dopiero edycja 2 z roku 2019 (EN 50600-1:2019) odbiła się szerszym echem na rynku polskim. Na innych rynkach europejskich sytuacja wyglądała różnie. Wyraźnie większe zainteresowanie wcześniejszą wersją normy było w Niemczech i Holandii. Można to uznać za zrozumiałe ponieważ w latach wcześniejszych były to wyraźnie przodujące rynki dla branży.

Obecnie nasz rynek rośnie dynamicznie co przekłada się również na zwiększone zainteresowanie dokumentami standaryzacyjnymi. W ramach prac KT 173 PKN wszystkie normy z serii EN 50600 uzyskują status polskich norm PN-EN.

Seria norm EN 50600 jest opracowywana i rozwijana przez grupę roboczą CENELEC TC 215 WG 03. Obecnie składa się z 20 zeszytów podzielonych na grupy tematyczne.

Tabela 1 – Struktura serii norm EN 50600.



1) raporty techniczne z serii CLC/TR 50600-99-x nie będą już rozwijane, ich funkcję przejmują inne zeszyty.

Seria norm EN 50600 wprowadziła zupełnie nową jakość do branży i stanowi:

- Źródło szeroko dostępnej i obiektywnej wiedzy dla inwestorów, projektantów i użytkowników,
- Podstawę do stworzenia bazy wytycznych dla projektantów,
- Dokumenty bazowe dla programu certyfikacyjnego dla fazy projektowej i wybudowanych obiektów.

oraz zawiera wskaźniki efektywności energetycznej dopasowane do obecnych wymagań.

Dowodem na duży i wciąż rosnący udział w rynku normy EN 50600 jest fakt, że coraz więcej centrów przetwarzania danych powstaje lub powstało w oparciu o wytyczne z EN 50600 zarówno w sferze kontraktów publicznych m.in. Centrum Informatyki Resortu Finansów w Radomiu, dwa obiekty Polskich Sieci Elektroenergetycznych S.A. jak również prywatnych.

Normy EN 50600 są także podstawą dla stworzenia wymagań niezwodnościowych dla budowy Krajowego Centrum Przetwarzania Danych. Jest to inwestycja strategiczna, która istotnie wpłynie na zapewnienie ciągłości działania systemów o krytycznym znaczeniu dla państwa[5].

Rada Ministrów w Uchwale z 11 września 2019 w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa" wprowadziła obowiązek zgodności z klasą 3 dostępności wg EN 50600 jako minimalne wymagania dla centrów przetwarzania danych przyłączonych do rządowej chmury obliczeniowej.

Niewątpliwie, **istotną wartością serii EN 50600 jest również wkład do Dyrektywy Parlamentu Europejskiego i Rady (UE) 2023/1791 w sprawie efektywności energetycznej (13 września 2023) wraz z Rozporządzeniem Delegowanym Komisji (UE) z dnia 14.3.2024 r. w sprawie pierwszego etapu ustanawiania wspólnego unijnego systemu oceny centrów przetwarzania danych wprowadzających obowiązek raportowania parametrów dla tych obiektów.** Większość wskaźników objętych raportowaniem jest zdefiniowanych w zeszytach EN 50600-4-x.

Równolegle, od 2016 roku, rozwija się seria norm ISO/IEC 22237 opracowywana przez grupę roboczą ISO/IEC JTC1 SC39 WG03. Seria ta jest w dużej części zbieżna z EN 50600. Drobne różnice występują ze względu na potrzebę uwzględnienia stanowisk ekspertów z innych części świata, które podyktowane są specyfiką tych rynków.
Jednakże, różnice te nie są istotne z punktu widzenia podejścia do rozwiązań technicznych. Wynika to m.in. z powodu, że praktycznie cała grupa ekspertów z Komisji Technicznej TC215 Cenelec uczestniczy w pracach ISO/IEC JTC1 SC39 WG03. Normy ISO/IEC 22237 obejmują swoim zakresem tematykę ujętą w zeszytach EN 50600-1, EN 50600-2-x, EN 50600-3-x. Natomiast odpowiednikiem zeszytów EN 50600-4-x są zeszyty ISO/IEC 30134-x.

Dla porządku należy wspomnieć o innych dokumentach normalizacyjnych funkcjonujących w branży. Na naszym rynku popularna jest i ma swój udział w rynku również norma ANSI TIA 942. Jednak, wraz ze wzrostem zainteresowania normami z grupy EN 50600 do normy tej przykłada się już mniej uwagi. Innym, amerykańskim standardem jest norma ANSI BICSI-002 „Data Center Design and Implementation Best Practices". Jest to dokument posiadający status normy niemniej na rynku polskim można go uznać za niszowy, znany raczej tylko ekspertom.

Niezależnie od mniejszego udziału w rynku obu normom nie można odmówić wartości merytorycznej. mają one zupełnie inną strukturę niż seria EN 50600.

Nie sposób też zapomnieć o modelu standaryzacji zaproponowanym już w latach 90 poprzedniego wieku przez Uptime Institute. Firma ta stworzyła, niewątpliwie podwaliny pod współczesną filozofię niezawodności i odporności centrów przetwarzania danych. Dokumenty Uptime Institute nie są jednak normami w formalnym tego słowa znaczeniu. Standardy Uptime Institute coraz rzadziej są używane na polskim rynku jako baza do tworzenia wytycznych dla centrów przetwarzania danych, co oczywiście nie przekreśla ich wartości merytorycznej.

Podsumowując, można bezsprzecznie stwierdzić, że grupa norma EN 50600 pełni dziś wiodącą rolę dla branżowego rynku centrów przetwarzania danych i rola ta będzie nadal rosła.

[4]wiecej o KCPD przeczytają Państwo na łamach tego raportu, w wywiadzie z Jackiem Siemionczykiem, zastepca dyrektora COI, jak również w case study dotyczącym tejże inwestycji.

3. REGULACJE DOTYCZĄCE DOSTĘPU DO DANYCH PRZEZ RZĄDY

JAKUB KULESZA

Forum Prawo do Rozwoju

Wymagania dotyczące dostępu do danych: Rządy niektórych krajów mogą wymagać dostępu do danych przechowywanych w centrach danych na podstawie przepisów dotyczących bezpieczeństwa narodowego, co może rodzić konflikty z przepisami ochrony prywatności.

Kontekst i wyzwania prawne

W dobie rosnących zagrożeń związanych z bezpieczeństwem narodowym, wiele rządów na całym świecie wprowadza przepisy, które umożliwiają im dostęp do danych przechowywanych w centrach danych na podstawie przepisów dotyczących bezpieczeństwa narodowego, walki z terroryzmem czy przestępczością. Te regulacje, choć zrozumiałe z punktu widzenia bezpieczeństwa, mogą prowadzić do poważnych konfliktów z przepisami o ochronie prywatności oraz z zasadami międzynarodowego prawa ochrony danych[1].

Przykłady regulacji na świecie

STANY ZJEDNOCZONE

Amerykański CLOUD Act (Clarifying Lawful Overseas Use of Data Act) to jedno z najbardziej znaczących ustaw, które regulują dostęp rządu do danych przechowywanych przez amerykańskie firmy technologiczne, niezależnie od tego, gdzie dane te fizycznie się znajdują. Ustawa ta pozwala amerykańskim organom ścigania na wydawanie nakazów dostępu do danych przechowywanych za granicą[2]. Może to jednak prowadzić do konfliktów z przepisami krajów, w których te dane są przechowywane, zwłaszcza w kontekście przepisów o ochronie danych osobowych, takich jak RODO (GDPR) w Unii Europejskiej[3].

UNIA EUROPEJSKA

W odpowiedzi na tego typu wyzwania, Unia Europejska pracuje nad regulacjami e-Evidence, które mają umożliwić organom ścigania dostęp do danych przechowywanych w innym kraju członkowskim UE. Projekt ten zmierza do stworzenia ram prawnych, które ułatwią wymianę danych między państwami członkowskimi, przy jednoczesnym zachowaniu wysokich standardów ochrony danych[6]. Niemniej jednak, jak pokazuje sprawa Schrems II, istnieje ryzyko, że dostęp rządowy do danych przechowywanych poza UE może naruszać prawo do prywatności obywateli[4].

Konflikty z przepisami o ochronie prywatności

Regulacje umożliwiające rządom dostęp do danych mogą kolidować z międzynarodowymi standardami ochrony danych, szczególnie w kontekście RODO, które stawia na pierwszym miejscu ochronę prywatności obywateli. Przykładem tego jest wspomniana wcześniej decyzja Trybunału Sprawiedliwości Unii Europejskiej w sprawie Schrems II, która unieważniła transatlantycki program Privacy Shield, umożliwiający transfer danych między UE a USA, z powodu obaw związanych z nadmiernym dostępem amerykańskich agencji rządowych do danych Europejczyków[4].

CHINY

W Chinach rządowe przepisy dotyczące dostępu do danych są jeszcze bardziej rygorystyczne. Chińskie prawo wymaga, aby różne formy danych, w tym dane osobowe, były przechowywane w Chinach, a ich transfer za granicę mógł nastąpić jedynie po przeprowadzeniu rządowej kontroli bezpieczeństwa. To podejście, znane jako „Beijing Effect", stanowi model zarządzania danymi, który koncentruje się na

ściślejszej kontroli państwa nad cyfrową infrastrukturą i przepływami danych[5].

Wpływ na rynek centrów danych

Regulacje te mają bezpośredni wpływ na rynek centrów danych, ponieważ zmuszają firmy do lokalizacji danych w konkretnych krajach, aby uniknąć konfliktów prawnych. Oznacza to, że operatorzy centrów danych muszą inwestować w lokalne infrastruktury, aby spełniać wymagania różnych jurysdykcji. Takie działania, choć zwiększają bezpieczeństwo danych, mogą prowadzić do fragmentaryzacji globalnego rynku cyfrowego oraz do wyższych kosztów operacyjnych. Przykładem tego jest wymóg, aby międzynarodowe firmy posiadały fizyczną infrastrukturę w krajach, gdzie świadczą usługi, co komplikuje zarządzanie globalnymi zasobami danych[5].

Rekomendacje i przyszłość regulacji

Przyszłość regulacji dotyczących dostępu rządowego do danych będzie prawdopodobnie nadal kształtowana przez rosnące obawy dotyczące bezpieczeństwa narodowego oraz potrzeby ochrony prywatności. Operatorzy centrów danych muszą być świadomi tych zmian i przygotowani na wdrażanie rozwiązań, które z jednej strony zapewnią zgodność z lokalnymi przepisami, a z drugiej strony ochronią prywatność użytkowników. W tym kontekście, **ważnym krokiem może być rozwój międzynarodowych ram prawnych, które zrównoważą potrzeby bezpieczeństwa z ochroną danych, umożliwiając jednocześnie swobodny przepływ informacji w skali globalnej[1].**

Podsumowując, **operatorzy centrów danych stoją przed wyzwaniem polegającym na znalezieniu równowagi między zgodnością z lokalnymi przepisami a ochroną prywatności swoich klientów.** Zmiany w regulacjach dotyczących dostępu do danych przez rządy będą miały długofalowy wpływ na strategię zarządzania danymi i rozwój globalnego rynku centrów danych.

[1]ASSESSING THE IMPLICATIONS OF SCHREMS II FOR EU–US DATA FLOW. Cambridge University Press, 2021 dostęp 29.08.2024 r.: https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/assessing-the-implications-of-schrems-ii-for-euus-data-flow/71E5412185BA0AE59B9F1AE1CFB6B97B
[2]Unpacking the CLOUD Act. Eucrim, 2018, dostęp 29.08.2024 r.: https://eucrim.eu/articles/unpacking-cloud-act/

[3]Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act. U.S. Department of Justice, 2019, dostęp 29.08.2024 r.: https://www.justice.gov/d9/pages/attachments/2019/04/10/doj_cloud_act_white_paper_2019_04_10.pdf
[4]Geopolitical Implications of the European Court's Schrems II Decision. Lawfare, 2020 dostęp 29.08.2024 r.: https://www.lawfaremedia.org/article/geopolitical-implications-european-courts-schrems-ii-decision
[5]EU tries to pin down China on definition of 'important data'. The Register, 2024, dostęp 29.08.2024 r.: https://www.theregister.com/2024/08/29/eu_china_data_talks/
[6]Łatwiejszy dostęp do e-dowodów – skuteczniejsza walka z przestępczością. Rada Europejska, Rada Unii Europejskiej, dostęp 29.08.2024 r.: https://www.consilium.europa.eu/pl/policies/e-evidence/

4. PRZEPISY DOTYCZĄCE OCHRONY PRZED KLĘSKAMI ŻYWIOŁOWYMI I PLANY AWARYJNE

JAKUB KULESZA
Forum Prawo do Rozwoju

Plany awaryjne i ciągłość działania: Operatorzy centrów danych muszą mieć plany awaryjne na wypadek klęsk żywiołowych, takich jak powodzie, pożary czy trzęsienia ziemi, aby zapewnić ciągłość działania.

Wprowadzenie

Ochrona przed klęskami żywiołowymi oraz zapewnienie ciągłości działania są kluczowymi elementami zarządzania centrami danych.

Wraz z rosnącą liczbą zagrożeń związanych z katastrofami naturalnymi, takimi jak powodzie, pożary, huragany czy trzęsienia ziemi, operatorzy centrów danych muszą opracowywać i wdrażać szczegółowe plany awaryjne oraz strategie ciągłości działania. Przepisy regulujące te kwestie są coraz bardziej rygorystyczne, szczególnie w branżach o dużej wrażliwości na przestoje, takich jak sektor finansowy, opieka zdrowotna czy usługi rządowe. W Polsce te aspekty są dodatkowo regulowane przez przepisy krajowe, co stawia przed operatorami dodatkowe wyzwania[1][2][3].

Znaczenie planów awaryjnych i ciągłości działania

W kontekście centrów danych plany awaryjne i strategie ciągłości działania mają na celu zminimalizowanie przestojów i ochronę integralności danych. Jest to szczególnie ważne w obliczu katastrof naturalnych, które mogą prowadzić do poważnych zakłóceń w działaniu centrów danych[2].

Skuteczne plany awaryjne obejmują:

- **Ocena ryzyka i analiza zagrożeń:** Identyfikacja potencjalnych zagrożeń, takich jak klęski żywiołowe, awarie zasilania, ataki cybernetyczne oraz inne incydenty mogące zakłócić działanie centrum danych. Analiza ta pozwala na stworzenie odpowiednich strategii, które minimalizują ryzyko.

- **Redundancja i replikacja danych:** Wdrażanie redundantnych systemów oraz technologii replikacji danych, co pozwala na szybkie odzyskiwanie krytycznych informacji i minimalizację strat danych. Ważnym elementem jest również geograficzne rozproszenie kopii zapasowych, aby zminimalizować ryzyko związane z jednoczesnym uszkodzeniem pierwotnej i zapasowej lokalizacji w przypadku dużego zdarzenia.

- **Testowanie i konserwacja planów:** Regularne testowanie planów awaryjnych jest kluczowe dla wykrycia potencjalnych luk i wzmocnienia gotowości na wypadek rzeczywistego zagrożenia. Procedury te obejmują symulacje sytuacji kryzysowych oraz aktualizacje planów zgodnie z nowymi zagrożeniami i technologiami.

Polskie regulacje dotyczące ochrony przed klęskami żywiołowymi

W Polsce przepisy dotyczące ochrony przed klęskami żywiołowymi oraz plany awaryjne są częściowo uregulowane przez prawo dotyczące ochrony danych osobowych, jak również przez przepisy związane z infrastrukturą krytyczną.

Ustawa o ochronie danych osobowych oraz RODO (Rozporządzenie o Ochronie Danych Osobowych) nakładają na operatorów centrów danych obowiązek zapewnienia odpowiednich środków technicznych i organizacyjnych w celu ochrony przetwarzanych danych. W kontekście klęsk żywiołowych oznacza to, że operatorzy muszą mieć plany awaryjne, które zapewnią bezpieczeństwo danych nawet w ekstremalnych warunkach[1].

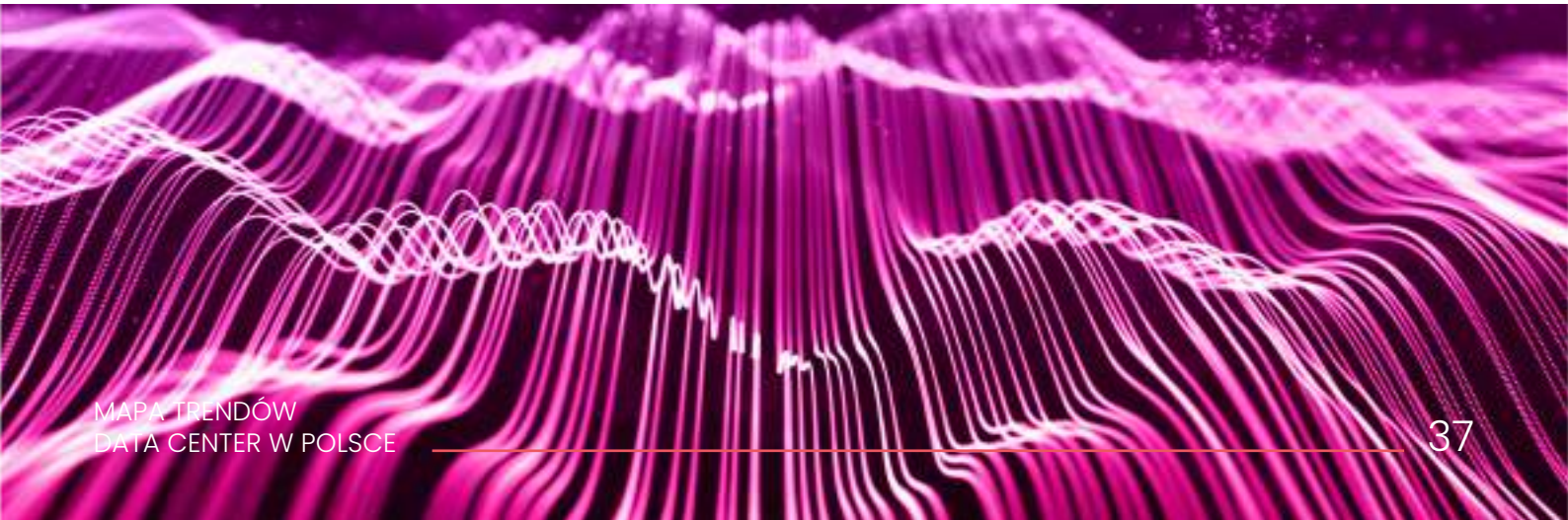
Przepisy te zobowiązują do:

- **Przeprowadzania oceny ryzyka związanego z klęskami żywiołowymi.**

- **Zastosowania środków zapobiegawczych, takich jak redundancja infrastruktury oraz regularne tworzenie i przechowywanie kopii zapasowych danych w lokalizacjach oddalonych od pierwotnych centrów danych.**

- **Regularnego testowania planów awaryjnych i ich dostosowywania do zmieniających się zagrożeń.**

Ustawa o zarządzaniu kryzysowym z 2007 roku, z późniejszymi nowelizacjami, dodatkowo nakłada na operatorów centrów danych obowiązek opracowania i utrzymania planów ciągłości działania[3].



Ustawa ta wymaga:

- **Opracowania szczegółowych planów działania na wypadek sytuacji kryzysowych, które uwzględniają scenariusze klęsk żywiołowych, takich jak powodzie czy pożary.**
- **Koordynacji działań z odpowiednimi organami państwowymi, takimi jak Rządowe Centrum Bezpieczeństwa (RCB), które nadzoruje zarządzanie kryzysowe w Polsce.**
- **Regularnej aktualizacji i testowania planów awaryjnych, aby były one zgodne z najnowszymi zagrożeniami i technologiami.**

Wytyczne branżowe i międzynarodowe standardy

W Polsce, zwłaszcza w sektorze finansowym, istnieją dodatkowe regulacje nakładane przez Komisję Nadzoru Finansowego (KNF). Przykładem mogą być wytyczne dotyczące zarządzania ryzykiem operacyjnym, które wymagają od instytucji finansowych posiadania szczegółowych planów awaryjnych oraz przeprowadzania regularnych testów odporności infrastruktury IT na różne zagrożenia, w tym klęski żywiołowe[4].

Dodatkowo, wiele polskich centrów danych wdraża międzynarodowe standardy, takie jak **ISO 22301, który definiuje wymagania dotyczące zarządzania ciągłością działania. Zgodność z tym standardem jest często wymagana w przetargach publicznych oraz w umowach z partnerami międzynarodowymi,** co zwiększa wiarygodność i zaufanie do oferowanych usług.

Wyzwania i rekomendacje

Dostosowanie się do wymogów związanych z ochroną przed klęskami żywiołowymi oraz zapewnieniem ciągłości działania jest dla operatorów centrów danych w Polsce istotnym wyzwaniem. Wymaga to nie tylko inwestycji w nowoczesne technologie i infrastrukturę, ale również ścisłej współpracy z organami regulacyjnymi oraz dostawcami usług. Wdrażanie takich rozwiązań jak geograficznie rozproszone kopie zapasowe, redundantne systemy zasilania i chłodzenia, a także zaawansowane mechanizmy replikacji danych jest kluczowe dla zminimalizowania ryzyka przestojów oraz utraty danych.
Wraz ze wzrostem liczby klęsk żywiołowych i zagrożeń cybernetycznych, plany awaryjne muszą być regularnie aktualizowane i testowane, aby sprostać nowym wyzwaniom. Dla firm operujących w Polsce kluczowe jest utrzymanie zgodności z lokalnymi przepisami, jednocześnie spełniając międzynarodowe standardy, co pozwala na budowanie zaufania wśród klientów i partnerów biznesowych.

Podsumowując, skuteczne zarządzanie ryzykiem klęsk żywiołowych w centrach danych jest niezbędne dla zapewnienia ciągłości działania, ochrony danych oraz zgodności z przepisami prawa. Operatorzy centrów danych muszą być przygotowani na różnorodne scenariusze awaryjne, wdrażając kompleksowe i elastyczne strategie, które zapewnią nieprzerwaną dostępność usług i minimalizację potencjalnych strat.

[1]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 (ogólne rozporządzenie o ochronie danych), dostęp 29.08.2024 r.: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A32016R0679
[2]Ustawa o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 r. Dziennik Ustaw, dostęp 29.08.2024 r.: https://www.dziennikustaw.gov.pl/DU/rok/2018/pozycja/1560
[3]Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym. Kancelaria Sejmu RP, dostęp 29.08.2024 r.: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20070890590
[4]Rekomendacja M dotycząca zarządzania ryzykiem operacyjnym w bankach. Komisja Nadzoru Finansowego, dostęp 29.08.2024 r.: https://www.knf.gov.pl/knf/pl/komponenty/img/Rekomendacja_M_8_01_2013_uchwala_8_33017.pdf

5. OCHRONA PRZED CYBERATAKAMI: WYMOGI TECHNOLOGICZNE I PROCEDURALNE DLA CENTRÓW DANYCH W OBLICZU ROSNĄCEJ LICZBY ZAGROŻEŃ

Izabela Taborowska
Prezeska, CyberClue

Wraz z rosnącą ilością i złożonością cyberataków, centra danych stają się kluczowym punktem koncentracji działań z zakresu bezpieczeństwa IT. Nowoczesne strategie ochrony muszą integrować zaawansowane technologie z dobrze zdefiniowanymi procedurami operacyjnymi, aby skutecznie zapobiegać nieautoryzowanemu dostępowi, kradzieży danych oraz atakom typu ransomware. Niniejsza analiza przedstawia kluczowe elementy tego podejścia, koncentrując się na aspektach technicznych i proceduralnych oraz kluczowych zabezpieczeniach.

Ewolucja Zagrożeń: Dynamika Cyberataków na Centra Danych

Wzrost liczby cyberataków, zarówno pod względem częstotliwości, jak i wyrafinowania, wymaga od operatorów centrów danych stałego dostosowywania strategii bezpieczeństwa. Według danych Enisa z 2023 roku, incydenty związane z naruszeniem integralności danych zwiększyły się o ponad 30% rok do roku, a ataki typu ransomware stały się bardziej zaawansowane, skutecznie omijając tradycyjne mechanizmy zabezpieczeń.
Centra danych, zarządzające ogromnymi wolumenami krytycznych danych są szczególnie narażone na te zagrożenia. Niezdolność do zapewnienia odpowiedniego poziomu ochrony może skutkować nie tylko bezpośrednimi stratami finansowymi, ale także naruszeniem zgodności z przepisami prawnymi i utratą zaufania klientów. Dlatego też konieczne jest wdrożenie kompleksowych mechanizmów ochrony, które będą skuteczne w walce z nowoczesnymi zagrożeniami cybernetycznymi.

Implementacja Zaawansowanych Technologii Ochronnych

Aby skutecznie przeciwdziałać cyberatakom, centra danych muszą korzystać z najnowszych osiągnięć technologicznych. Kluczowymi komponentami infrastruktury ochronnej stają się tu sztuczna inteligencja (AI), uczenie maszynowe (ML) oraz zaawansowana analiza Big Data. Technologie te umożliwiają nie tylko szybką identyfikację anomalii w ruchu sieciowym, ale także proaktywne zapobieganie potencjalnym zagrożeniom.

Poniżej przedstawiamy kluczowe zabezpieczenia, które powinny zostać zaimplementowane w nowoczesnych serwerowniach:

- Zapory Sieciowe (Firewalls): Zapory sieciowe kontrolują ruch sieciowy, blokując nieautoryzowane połączenia i przepuszczając jedynie ruch spełniający określone reguły bezpieczeństwa. Zapory te działają na różnych poziomach, w tym aplikacyjnym (WAF) i sieciowym (NGFW), chroniąc przed atakami typu DDoS oraz innymi zagrożeniami.

- Systemy Wykrywania i Zapobiegania Włamaniom (IDS/IPS): IDS wykrywają nieautoryzowane działania w sieci, podczas gdy IPS dodatkowo automatycznie reagują na wykryte zagrożenia, np. poprzez blokowanie podejrzanego ruchu lub izolowanie zainfekowanego urządzenia. Systemy te umożliwiają analizę ruchu sieciowego w czasie rzeczywistym oraz natychmiastową reakcję na incydenty.

- Segmentacja Sieci: Segmentacja sieci polega na podzieleniu infrastruktury na odseparowane segmenty, co utrudnia intruzom przemieszczanie się po sieci. Mikrosegmentacja, jako bardziej zaawansowana forma, umożliwia precyzyjne kontrolowanie ruchu między segmentami, zwiększając bezpieczeństwo wewnętrzne.

- Systemy Szyfrowania Danych: Szyfrowanie jest kluczowym elementem ochrony danych, zarówno podczas ich przechowywania, jak i przesyłania. Stosowanie algorytmów szyfrowania, takich jak AES-256, wraz z zarządzaniem kluczami opartym na PKI, zapewnia integralność i poufność danych.

- Zarządzanie Tożsamością i Dostępem (IAM): IAM zapewnia kontrolę dostępu do zasobów na podstawie tożsamości użytkownika oraz jego uprawnień. Systemy te umożliwiają precyzyjne zarządzanie dostępem do danych i aplikacji, uwzględniając kontekst, taki jak lokalizacja czy czas, co zwiększa bezpieczeństwo operacyjne.

- Systemy Kopii Zapasowych i Odzyskiwania Danych (Backup and Disaster Recovery): Regularne tworzenie kopii zapasowych oraz dobrze

zaprojektowane plany odzyskiwania danych po awarii są kluczowe dla minimalizacji skutków ataków ransomware. Kopie zapasowe powinny być przechowywane w izolowanych środowiskach, z dala od głównej infrastruktury.

- Ochrona Fizyczna: Zapewnienie fizycznego bezpieczeństwa serwerowni obejmuje kontrolę dostępu do budynków, monitorowanie pomieszczeń za pomocą kamer, systemy alarmowe oraz ograniczenie dostępu do krytycznych zasobów tylko dla autoryzowanego personelu.

- Systemy Detekcji i Ochrony przed Zagrożeniami na Poziomie Endpointów (EDR): EDR monitorują aktywność na urządzeniach końcowych, takich jak serwery i stacje robocze, identyfikując i reagując na zagrożenia w czasie rzeczywistym. Te systemy są kluczowe w ochronie przed zaawansowanymi zagrożeniami, takimi jak ataki zero-day.

- Analiza Ruchu Sieciowego (NTA): NTA analizuje ruch sieciowy w celu wykrycia anomalii, takich jak nieautoryzowane skanowanie portów lub nietypowy ruch, który może wskazywać na próbę ataku. W połączeniu z AI, NTA może automatycznie identyfikować i reagować na zagrożenia.

- Zarządzanie Zdarzeniami Bezpieczeństwa i Informacjami (SIEM): SIEM integruje i analizuje logi z różnych elementów infrastruktury IT, pozwalając na korelację zdarzeń i wykrycie złożonych ataków. Systemy SIEM umożliwiają także generowanie raportów i alarmów w czasie rzeczywistym, co jest kluczowe dla skutecznego zarządzania bezpieczeństwem.

Zintegrowane Procedury Ochronne i Reagowania na Incydenty

Ochrona techniczna, nawet najbardziej zaawansowana, nie jest skuteczna bez odpowiednich procedur operacyjnych. Wzrost liczby zagrożeń wymusza na centrach danych implementację kompleksowych polityk bezpieczeństwa, które obejmują zarówno prewencję, jak i skuteczną reakcję na incydenty.

- Regularne Audyty Bezpieczeństwa: Regularne audyty i testy penetracyjne są niezbędne do identyfikacji i eliminacji luk w zabezpieczeniach. Zautomatyzowane narzędzia skanowania podatności oraz ręczne audyty powinny być przeprowadzane cyklicznie, aby zapewnić, że infrastruktura jest odporna na najnowsze zagrożenia.

- Szkolenia i Testy Red Team: Przeszkolenie personelu w zakresie bezpieczeństwa IT oraz regularne testy Red Team, symulujące ataki na infrastrukturę, są kluczowe dla zapewnienia, że zespół IT jest przygotowany na rzeczywiste zagrożenia. Dzięki takim działaniom pracownicy są w stanie szybko i skutecznie reagować na incydenty, minimalizując ryzyko eskalacji ataków.

- Plan Reagowania na Incydenty (IRP): Każde centrum danych musi posiadać dobrze zdefiniowany plan reagowania na incydenty (Incident Response Plan), który precyzuje kroki działania w przypadku wykrycia naruszenia bezpieczeństwa. Plan ten powinien obejmować zarówno działania techniczne, takie jak izolacja zainfekowanych segmentów sieci, jak i komunikacyjne, w tym powiadomienie klientów, regulatorów oraz wewnętrznych interesariuszy.

Przyszłość Zabezpieczeń w Centrach Danych

Ewolucja zagrożeń wymaga, aby centra danych stale dostosowywały swoje strategie obronne. W najbliższych latach przewiduje się dalszy rozwój technologii opartych na AI i ML, które będą zdolne do bardziej zaawansowanej analizy i automatyzacji reakcji na zagrożenia. Ponadto, migracja do środowisk chmurowych i rozwój architektur hybrydowych będą wymagały wdrożenia nowych metod ochrony, które będą efektywnie działały w złożonych, rozproszonych infrastrukturach.

Podsumowując, rosnąca liczba i złożoność cyberataków wymaga od centrów danych nieustannego podnoszenia poziomu zabezpieczeń. Wdrożenie zaawansowanych technologii oraz zintegrowanych procedur ochronnych jest kluczowe dla zapewnienia ciągłości działania oraz ochrony danych. Tylko holistyczne podejście do cyberbezpieczeństwa, obejmujące zarówno technologie, jak i procesy, pozwoli na skuteczną obronę przed nowoczesnymi zagrożeniami.

3E PRZEWIDYWANIA DOTYCZĄCE PRZYSZŁOŚCI RYNKU DATA CENTER W POLSCE ORAZ POTENCJALNE WYZWANIA I MOŻLIWOŚCI DLA FIRM DZIAŁAJĄCYCH W TEJ BRANŻY

Adam Wnorowski
Instytut Transformacji

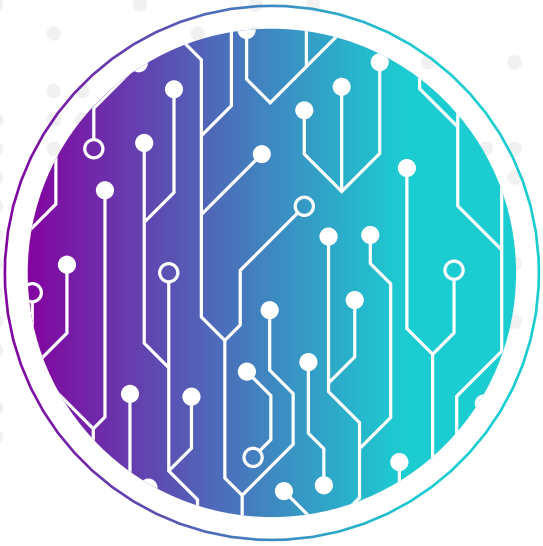
Obecnie polski rynek data center rośnie najszybciej w swej historii. Lata 2014-2018 można śmiało nazwać latami stagnacji. Od roku 2019 nastąpił systematyczny wzrost, na który składa się trend działań bezpośrednich i pośrednich.

Do bezpośrednich możemy zaliczyć migracje urządzeń przez firmy z własnych serwerowni do profesjonalnych obiektów, wejście na rynek światowych gigantów (polskie regiony chmur publicznych) oraz dobra koniunktura i zasobne portfele Polaków gotowych wydawać na usługi content digital media (platformy streamingowe, VOD, social media).

W pośrednich znajdziemy wojnę w Ukrainie i potrzebę migracji infrastruktury w bezpieczniejsze lokalizacje dla ciągłości działania, ale także problemy z energią oraz zezwoleniami w tzw. Krajach FLAP-D (Frankfurt, Londyn, Amsterdam, Paryż i Dublin). Prognozowany przez firmę PMR wzrost dostępnej mocy data center to około 500MW jest mocno prawdopodobny. Być może zostanie on przekroczony dzięki kolejnemu wyścigowi na rynku sztucznej inteligencji.

Polska – ze swoim ogromnym potencjałem w postaci mocno wykwalifikowanej kadry IT – jest w stanie mocno 'namieszać' na rynku i awansować z grupy globalnych rynków Tier II do Tier I (właśnie FLAP-D).

Instytut Transformacji ma w swoim DNA wsparcie rynku data center oraz energii celem zapewnienia odpowiednich zapisów i regulacji, które pozwolą na zapewnienie odpowiedniej ilości zielonej energii oraz gruntów pod wzrost sektora centrów danych w synergii z nowymi źródłami OZE.



Jeszcze kilka lat temu Polska mogła pochwalić się jednym z najniższych kosztów energii elektrycznej, która jest krwią obiektów data center. Obecnie znaleźliśmy się na drugim końcu w skali globalnej i jest to sytuacja, która zdecydowanie utrudnia rozwój w tempie podobnym do kilku ostatnich lat. Tym bardziej jest to istotne, aby wykorzystać obecny moment i zapotrzebowanie na rozwiązania AI. W porównaniu z rozwiązaniami typu cloud compute, w których gęstość mocy na szafę wynosiła średnio 4-8kW, infrastruktura sztucznej inteligencji obecnie potrzebuje minimum 30kW, coraz częściej 60kW, a nawet – w skrajnych przypadkach najdroższych dostępnych technologii – 130kW na jedną szafę.

Niesie to za sobą wyzwania, ale także dodatkowe możliwości. Dotychczas typowe obiekty powstawały na działkach 4-6 ha i mocy rzędu 30-60MW. Obiekty na potrzeby AI mogą zajmować działki o połowę mniejsze, ale ich zapotrzebowanie na moc – dwukrotnie większe, a więc nawet 120MW. Przy obecnym, przeciążonym systemie sieci energetycznych jest to nie lada wyzwanie.

W obliczu wyzwań stojących przed branżą data center, firmy muszą wdrażać innowacyjne rozwiązania, które przyniosą trwałe korzyści. Jednym z kluczowych kierunków może być stworzenie synergii między sektorami: energetycznym, data center oraz ciepłowniczym. Jednym z nich może być zapewnienie synergii branż: energetyka-data center-ciepłownictwo.

Rozważenie i**ntegracji zielonej energii (OZE, SMR) z infrastrukturą data center** mogłoby przynieść znaczące korzyści zarówno ekonomiczne, jak i ekologiczne. Umieszczenie farm fotowoltaicznych, turbin wiatrowych lub innych źródeł OZE, a także **małych reaktorów modułowych (SMR, Small Modular Reactors)** na tej samej działce co data center, pozwoliłoby na bezpośrednie wykorzystanie produkowanej energii (a w przypadku SMR również zapewnienia ciągłości działania). Taka strategia nie tylko przyczyniłaby się do obniżenia kosztów operacyjnych związanych z zasilaniem i chłodzeniem, ale także znacznie zredukowałaby ślad węglowy, odpowiadając na rosnące wymagania dotyczące zrównoważonego rozwoju.

Na drugim końcu tej synergii mamy **odzysk ciepła z data center.** Centra danych generują znaczące ilości ciepła odpadowego, które może być efektywnie wykorzystane do ogrzewania pobliskich budynków, a nawet większych obszarów miejskich. Wprowadzenie takich rozwiązań umożliwiłoby data center pełnienie kluczowej roli w lokalnych systemach energetycznych, przyczyniając się do zwiększenia efektywności energetycznej na poziomie całego miasta. Takie rozwiązania już funkcjonują: Meta w Odense (Dania), AWS w Dublinie (Irlandia) oraz Microsoft w Espooand Kirkkonummi (Finlandia).

Synergia między data center a zieloną infrastrukturą energetyczną, w tym wykorzystaniem SMR, OZE oraz systemów odzysku ciepła, stanowi zatem nie tylko inwestycję w przyszłość sektora, ale także w zrównoważony rozwój gospodarki i społeczeństwa. Przyjęcie takiej strategii będzie kluczowe dla uzyskania przewagi konkurencyjnej i umocnienia pozycji Polski na europejskim rynku usług data center.

Widzimy znaczny wzrost zainteresowania wielu firm, tworzących ekosystem wokół branży data center, które chcą dostosować swoje usługi pod potrzeby na najbliższe lata. W Polsce mamy doświadczonych ludzi, uznane firmy i know-how aby odpowiednio przygotować się na realizację prognoz dla tego sektora. Przyszłość rysuje się w jasnych barwach a zainteresowanie Polską zdaje się nie maleć.

6. WYWIADY

6.1 JACEK SIEMIOŃCZYK

CENTRALNY OŚRODEK INFORMATYKI
– ZASTĘPCA DYREKTORA

Boom na AI zaskoczył wszystkich, także operatorów Data Center. Co może wpłynąć równie silnie na podaż centrów danych po AI?

Mam wrażenie, że boom na AI nie był zaskoczeniem dla największych operatorów na świecie. Mógł być zaskoczeniem dla operatorów lokalnych, i tam ograniczeniem stało się to, że brakowało jednostek do przetwarzania obliczeń związanych ze sztuczną inteligencją. Ale to wynikało z tego, że osiągnięto pułap mocy produkcyjnych u największych dostawców, jak Nvidia czy AMD. Najwięksi operatorzy Data Center na świecie, ze względu na swoją skalę działalności, zmonopolizowali nieco podaż produkcji, wykupując na pniu rozwiązania GPU oferowane przez firmy. Mniejsze ośrodki przetwarzania danych miały wtedy trudności z dostępem do mocy obliczeniowej, aby oferować rozwiązania AI swoim klientom. Nie jestem przekonany, że było tak, że to lokalni gracze nie doszacowali zapotrzebowania na moc obliczeniową.

Czy na horyzoncie jest jakaś zmiana?

Nie przeszacowywałbym komputerów kwantowych, przynajmniej nie na bliskim horyzoncie. Jednocześnie nie widzę niczego, co mogłoby mieć tak duży wpływ na rynek jak AI. AI zmieniło rynek kolosalnie z wielu powodów. Wiele firm chce za wszelką cenę wykorzystać sztuczną inteligencję, chociaż nie zawsze wiedzą jeszcze jak to zrobić. Ale robią to, licząc, że na uzyskanie przewagi konkurencyjnej. Nie widzę jednak na horyzoncie podobnej zmiany.

Rozwiązania sztucznej inteligencji zmieniły wiele kwestii w wykorzystaniu Data Center, jak np. gigantyczny wzrost zapotrzebowania na przestrzeń dyskową. To zmieniło charakterystykę usług, którymi trzeba umieć zarządzać.
Zapotrzebowanie na przestrzeń dyskową może być trendem, który wpłynie na strukturę centrów przetwarzania danych. Pojawia się wzrost zainteresowania edge computing, co może wpłynąć na rozwój małych ośrodków przetwarzania danych, które wspomogą procesy filtrowania danych, które trafiają do centrów przetwarzania. Wierzę również, że sztuczna inteligencja pomoże w zarządzaniu mocą obliczeniową, która nie jest nieskończona, ale dzięki algorytmom opartym o AI można ją efektywniej wykorzystywać.

Jakie trendy ekologiczne w branży data center uważa Pan za najważniejsze w najbliższych latach?

Świadomość ekologiczna jest różna w różnych częściach świata, ale uważam, że przejście na energię ze źródeł odnawialnych, redukowanie emisji, minimalizacja zużycia wody oraz angażowanie się w projekty ekologiczne będą kluczowe. Projekty rewitalizacji terenów czy budowa zbiorników retencyjnych będą się rozwijały, ale głównie w krajach o bardziej rozwiniętej gospodarce. W krajach rozwijających się nadal większe znaczenie będzie miała ekonomia i bezpieczeństwo danych.
Przejście na energię odnawialną jest nie tylko kwestią marketingową, ale ma także podłoże ekonomiczne. Wzrost kosztów energii ze źródeł nieodnawialnych wymusi poszukiwanie alternatyw. W perspektywie pięciu lat nie spodziewam się przełomu w wykorzystania energii jądrowej, ale wiatrowa, słoneczna czy wykorzystanie napędów wodorowych, będą się rozwijać.
W Stanach Zjednoczonych czy Europie Zachodniej ekologia ma wymiar praktyczny i rzeczywisty, co powoduje, że firmy tam działające przykładają większą wagę do ekologicznych rozwiązań. W Polsce również są podejmowane kroki w tym kierunku, np. w ramach projektu KCPD, gdzie część zasilania będzie pochodziła ze źródeł odnawialnych. Energia odnawialna, choć postrzegana jako ekologiczna, ma również wymiar ekonomiczny, szczególnie w kontekście wzrostu kosztów energii z nieodnawialnych źródeł.
Ponadto, najwięksi z dostawców rozwiązań Data Center angażują się w projekty związane z rekultywacją gruntów, zmniejszeniem erozji czy budową zbiorników retencyjnych, co pokazuje rosnące zaangażowanie w zrównoważony rozwój.

Jakie inwestycje i/lub nowe usługi planujecie wprowadzić, aby sprostać przyszłym wyzwaniom i trendom na rynku?

Projekt Krajowego Centrum Przetwarzania Danych (KCPD) jest strategiczny. Budowa suwerennej chmury pozwoli Polsce być niezależnym od dużych dostawców chmury publicznej. KCPD umożliwi cyfryzację całej Polski, dostarczając wysoko wydajne, bezpieczne rozwiązania.
Centralny Ośrodek Informatyki (COI) planuje zbudowanie technologicznego hubu AI dla administracji publicznej. W perspektywie chcemy, aby COI stało się takim centrum kompetencyjnym wspierającym rozwój i adopcję rozwiązań opartych o sztuczną inteligencję, co wymagać będzie zbudowania suwerennej chmury oraz skalowalnych środowisk produkcyjnych.

Jakie są Państwa długoterminowe cele strategiczne?

Nasze cele strategiczne są proste: cyfryzacja procesów między obywatelami a administracją publiczną, eliminacja procesów papierowych oraz budowa chmury obliczeniowej w ramach KCPD. Chcemy, aby aplikacja mObywatel stała się głównym wejściem do większości procesów administracyjnych.

Jakie zmiany zauważacie Państwo w preferencjach klientów dotyczących usług data center?

Preferencje klientów zmieniają się w kierunku ekologii i efektywności energetycznej, ale największym priorytetem pozostaje wysoka dostępność i cyberbezpieczeństwo. Administracja publiczna, szczególnie mniejsze ośrodki, potrzebuje dostępu do wysoko dostępnych, bezpiecznych usług, co KCPD może zapewnić.

6.2 ANNA STREŻYŃSKA

PRZEWODNICZĄCA KOMITETU TECHNOLOGII KWANTOWYCH, KRAJOWA IZBA GOSPODARCZA

W jaki sposób Quantum Computing może mieć wpływ na branżę data center w przyszłości?

Informatyka kwantowa jest jeszcze dziedziną niedojrzałą, ale szybko się rozwija, także w Polsce. Należy jednak wyróżnić dwie prędkości rozwoju: różne technologie kwantowe oparte na fizyce kwantowej, często służące już optymalizacji różnych procesów (np. sensing) od czystej informatyki, która także składa się z dwu ścieżek o różnych prędkościach – software'u i hardware'u. Zgodnie z raportami, do końca 2022 roku zainwestowano 5,4 miliarda dolarów w technologie kwantowe, a na rynku globalnym działało około 223 startupów. McKinsey prognozuje, że rynek technologii kwantowej może osiągnąć wartość 106 miliardów dolarów do 2040 roku.

Quantum computing przyniesie korzyści w takich dziedzinach jak finanse, farmacja, logistyka, bezpieczeństwo i obrona, umożliwiając bardziej zaawansowane analizy i symulacje, skracając i optymalizując złożone procesy badawcze i logistyczne.

Sztuczna inteligencja, która nas teraz bardzo interesuje, także oczekuje na kwantową wydajność obliczeń kwantowych w przetwarzaniu danych, szczególnie w przypadku zastosowań takich jak analiza dużych zbiorów danych i złożone symulacje. Kwantowe przetwarzanie języka naturalnego (QNLP) zapewni postęp w eksploracji tekstu, automatyzacji dialogu,

tłumaczeniach ale co szczególnie przyszłościowe - także w bioinformatyce. Kwantowe uczenie maszynowe przyspieszy rozpoznawanie wzorców i procesy decyzyjne.

Branża data center, oferująca usługi kolokacyjne i cloud computing, w przyszłości stanie przed wyzwaniem połączenia obliczeń kwantowych z infrastrukturą tradycyjną, w tym chmurową, by umożliwić zdalny dostęp biznesu i nauki do zasobów kwantowych bez posiadania kwantowych maszyn i specjalistycznego sprzętu oraz oprogramowania, a także umożliwi w przestrzeni centrów danych integrację kwantowej infrastruktury komputerowej z tradycyjnymi zasobami baz danych i sieciami telekomunikacyjnymi. Dzięki temu posiadacze kwantowych maszyn obliczeniowych nie będą musieli budować własnych obiektów.

Zanim to nastąpi, kluczowe będzie rozwinięcie wszechstronnej współpracy operatorów centrów danych z producentami komputerów kwantowych oraz inwestycje w badania i rozwój. Wiele światowych instytucji akademickich i firm technologicznych prowadzi już intensywne badania nad technologią kwantową i jej zastosowaniami w centrach danych.

Ciekawym przykładem jest izraelskie Quantum Computing Center (IQCC) które integruje różne typy komputerów kwantowych z tradycyjnymi superkomputerami, wykorzystując system NVIDIA DGX Quantum do ultraszybkiej komunikacji. Ponadto centrum dysponuje najlepiej wyposażonym na świecie poligonem doświadczalnym do opracowywania nowych technologii obliczeń kwantowych, oferując szeroki dostęp do środowiska akademickiego i przemysłu. Israeli Quantum Computing Center wdraża „trójwymiarową" przyszłość centrum danych: tradycyjne procesory ściśle zintegrowane z systemami AI i akceleratorami kwantowymi.

Oczywiście, ważne będą także regulacje stosowane w tej dziedzinie, nie tylko te klasyczne, jak cyberbezpieczeństwo, Data Act, RODO, ale także te dziedzinowe, szczególnie w zakresie standaryzacji: specyfikacje dotyczące zasilania, chłodzenia, zarządzania kablami oraz zabezpieczeń fizycznych, nowe standardy szyfrowania i zabezpieczeń, które będą odporne na ataki kwantowe, protokoły komunikacyjne, interfejsy sprzętowe i oprogramowanie, które umożliwią płynną integrację technologii klasycznej i kwantowej, oraz inne wymagania w zakresie modernizacji istniejących centrów danych oraz budowy nowych obiektów dostosowanych do wymagań komputerów kwantowych.

Na tym z kolei tle bardzo ważna jest współpraca środowiska z organizacjami standaryzacyjnymi: ISO (International Organization for Standardization), ITU (International Telecommunication Union) i IEEE (Institute of Electrical and Electronics Engineers).

Środowisko data center będzie też musiało powalczyć z wyzwaniami technologicznymi, o czym zaraz opowiem.

Czy komputery kwantowe mogą znacząco zwiększyć efektywność przetwarzania danych w data center? Jeśli tak, w jaki sposób?

Technologie kwantowe w zasadzie wyłącznie po to istnieją i dla data center będzie to prawdziwa, ale pozytywna rewolucja. Dzięki właściwościom technologii świat przetwarzania danych zupełnie się odmieni. Superpozycja czyli fakt że qubity mogą istnieć w wielu stanach jednocześnie, pozwoli na równoczesne przetwarzanie wielu możliwości, tez badawczych czy kierunków analitycznych. Splątanie qubitów czyli ich natychmiastowy wpływ na siebie nawzajem przyspiesza procesy obliczeniowe. Quantum parallelism (równoległość kwantowa) umożliwia eksplorację wielu potencjalnych rozwiązań jednocześnie. Generalnie komputery kwantowe mogą znacznie przyspieszyć obliczenia, co jest szczególnie przydatne w kryptografii ale i innych zaawansowanych zastosowaniach, zarówno naukowych jak i biznesowych.

Komputery kwantowe (zgodnie z obietnicą, którą reprezentują, bo obecnie jeszcze jest do tego daleka droga) będą rozwiązywać problemy, które są zbyt skomplikowane dla klasycznych komputerów. Umożliwią rozwiązanie złożonych zagadnień w różnych dziedzinach, takich jak farmacja, modelowanie finansowe i sztuczna inteligencja. Wykonają swoją pracę przy znacznie mniejszym zużyciu energii niż klasyczne komputery. Przyspieszą algorytmy uczenia maszynowego i optymalizacji, co poprawia wydajność operacyjną data center.

Komputery kwantowe będą efektywnie przetwarzać i analizować ogromne zbiory danych, niedostępne dla współczesnych systemów z uwagi na czas obliczeń, zatem zmienią jakość i zakres usług data center. Zaoferują zwiększoną dokładność w analizie danych, co jest szczególnie ważne w dziedzinach takich jak finanse, medycyna czy badania naukowe. Wszystko to przed nami, zakładając, że rozwiążemy największe problemy samej technologii.

Jakie konkretne problemy w centrach danych mogą być rozwiązane dzięki technologii kwantowej?

Już nieco o tym powiedzieliśmy, natomiast warto podkreślić, że główną cechą komputerów kwantowych jest zwiększona wydajność przetwarzania danych. Ogromne zbiory danych mogą być przetwarzane znacznie szybciej niż tradycyjne komputery, co daje mniej opóźnień i szybszy dostęp do informacji (nawet podobno docelowo wiele milionów razy szybszy) a dodatkowo złożoność problemów dostępna dla komputerów kwantowych jest obecnie nieosiągalna dla klasycznych komputerów.

Dzięki zaawansowanym algorytmom kwantowym, centra danych będą mogły lepiej zarządzać własnymi zasobami, co prowadzi do oszczędności energii i pozostałych kosztów. Quantum computing może znacznie poprawić zarządzanie zasobami sprzętowymi, takimi jak moc obliczeniowa i przestrzeń dyskowa.

Technologia kwantowa wprowadzi nieuchronnie nowe metody szyfrowania, które są znacznie trudniejsze do złamania, zwiększając bezpieczeństwo przechowywanych danych.

Jak zawsze, żeby dojść do tych wyników efektywnościowych, najpierw trzeba będzie zainwestować.

Jakie są główne wyzwania technologiczne związane z integracją komputerów kwantowych z tradycyjnymi data center?

Jest ich cały szereg. Tradycyjne data center są zaprojektowane do pracy z klasycznymi komputerami, więc integracja z komputerami kwantowymi wymaga dostosowania infrastruktury i zapewnienia kompatybilność sprzętowej. Centra danych muszą dostosować swoje systemy zasilania, chłodzenia oraz zabezpieczenia fizyczne, aby sprostać wymaganiom komputerów kwantowych. Obejmuje to zaawansowane systemy chłodzenia kriogenicznego oraz zarządzanie płynami kriogenicznymi. Komputery kwantowe wymagają ekstremalnie niskich temperatur do działania, co oznacza konieczność zastosowania zaawansowanych systemów chłodzenia, które nie są standardem w tradycyjnych data center. Quantum computing jest bardzo wrażliwy na zakłócenia elektromagnetyczne, które są powszechne w tradycyjnych data center. Te dwie kwestie są ważne dla stabilności qubitów.

A zatem kolejne problemy to dźwięk i ekranowanie elektromagnetyczne, przestrzeń (są duże) i łączność (komputery kwantowe wymagają szybkich połączeń o niskim opóźnieniu, aby przesyłać dane do i z komputera).

Ponieważ quantum computing i klasyczne komputery mają różne architektury sprzętowe, integracja tych dwóch technologii wymaga opracowania nowych interfejsów i protokołów komunikacyjnych, o czym już wspomniałam.

Komputery kwantowe często wymagają szybkich połączeń o niskim opóźnieniu, aby przesyłać dane do i z komputera.

Oczywiście dochodzą do tego problemy immanentnie związane z samą technologią, w tym korekcja błędów kwantowych (obliczenia kwantowe są podatne na błędy, co wymaga rozwinięcia zaawansowanych metod korekcji błędów), skalowalność systemów kwantowych (budowa i utrzymanie dużych systemów kwantowych z tysiącami kubitów stanowi znaczące wyzwanie techniczne i logistyczne. Obecne technologie kwantowe mają trudności z skalowaniem liczby kubitów, co jest niezbędne do osiągnięcia pełnej funkcjonalności w dużych data center) oraz koszty i dostępność (wdrożenie technologii kwantowej wiąże się z wysokimi kosztami, zarówno w zakresie sprzętu, jak i infrastruktury wspierającej). Jednak to będzie dotyczyć data center tylko wtedy, gdy usługi oferowane przez nie będą wykraczać poza standardową kolokację i połączenie sprzętu i sieci.

Nie sposób zapomnieć o pracownikach: kluczowe jest rozwijanie umiejętności i wiedzy pracowników, aby skutecznie zarządzać taką infrastrukturą. Zarówno operatorzy centrów danych, jak i dostawcy komputerów kwantowych będą musieli dostosować się do nowych wymagań i procedur zintegrowanego środowiska.

Dla realizacji biznesu kluczowy będzie dostęp do ekosystemu: Bezpośredni dostęp nie tylko do przedsiębiorstw, ale także platform chmurowych. Łatwa integracja dla programistów i dostawców oprogramowania

W jaki sposób komputery kwantowe mogą wpłynąć na bezpieczeństwo danych przechowywanych w data center?

Komputery kwantowe mogą znacząco wpłynąć na bezpieczeństwo danych w centrach danych na kilka sposobów. Najważniejsze jest oczywiście szyfrowanie kwantowe. Komputery kwantowe mogą zarówno łamać powszechnie stosowane algorytmy szyfrowania jak i tworzyć nieprzełamywalne klucze szyfrujące, nowe

algorytmy odporne na ataki kwantowe, chroniące dane przed przyszłymi zagrożeniami. Wprowadzenie technik kryptografii kwantowej, takich jak Quantum Key Distribution (QKD), może zapewnić teoretycznie niełamliwe szyfrowanie. Dzięki QKD, każda próba podsłuchu transmisji klucza jest natychmiast wykrywana, co zapewnia wysoki poziom bezpieczeństwa.

Quantum computing może również pomóc w tworzeniu bardziej zaawansowanych algorytmów do wykrywania i zapobiegania atakom na dane. Dzięki swojej mocy obliczeniowej, komputery kwantowe mogą analizować ogromne ilości danych w czasie rzeczywistym, identyfikując potencjalne zagrożenia szybciej i dokładniej. Quantum computing może również przyczynić się do rozwoju nowych metod przechowywania danych, które są bardziej odporne na ataki i zapewniają wyższy poziom integralności danych.

Komputery kwantowe mogą także szybciej analizować duże ilości danych, co pozwala na szybsze wykrywanie i reagowanie na próby włamań. Technologia kwantowa może też zapewnić bezpieczne kanały komunikacji, eliminując ryzyko podsłuchu. Te technologie rozwijane są intensywnie także w Polsce.

A jakie są społeczne korzyści z przejścia na technologie kwantowe w data center?

Tradycyjne superkomputery mogą zużywać tyle energii, co małe miasteczko. W 2020 roku technologie informacyjne odpowiadały za 11% globalnego zużycia energii elektrycznej. Branża centrów danych odpowiada za około 4% światowego zużycia energii elektrycznej. Teoretyczne obliczenia sugerują, że komputery kwantowe mogą zużywać nawet sto razy mniej energii niż najlepsze superkomputery, przy porównywalnym czasie obliczeń. Quantum computing może pomóc w bardziej efektywnym zarządzaniu energią w czasie rzeczywistym, co jest kluczowe dla optymalizacji zużycia energii w dużych centrach danych. Szybsze przetwarzanie danych, optymalizacja algorytmów, redukcja liczby operacji, a wreszcie kwantowe symulacje i modelowanie pozwolą na lepsze planowanie i zarządzanie zasobami energetycznymi

Mniej znanym aspektem wpływu IT na środowisko jest zapotrzebowanie na wodę. Moja studnia w ogrodzie całkowicie wyschła co powoduje moje znaczne zainteresowanie gospodarką wodną. Ciepło generowane przez centra danych oznacza, że muszą być one stale chłodzone, a do tego celu często wykorzystuje się wodę.

Sukces generatywnej sztucznej inteligencji pogłębia ten problem i możemy znaleźć informacje autoryzowane przez badaczy, że na każdą serię od 5 do 50 pytań przesłanych do ChatGPT zużywa się około pół litra wody. W swoim najnowszym raporcie środowiskowym Microsoft ujawnił, że między 2021 a 2022 r. jego globalne zużycie wody wzrosło o 34%. W tym samym okresie Google odnotowało 20% wzrost zużycia wody. Jeśli komputery kwantowe spełnią pokładane w nich nadzieje, to rozwiążą także złożone problemy związane z optymalizacją zarządzania ciepłem w centrach danych. Zmniejszyłoby to zależność od klimatyzacji chłodzonej wodą, oszczędzając znaczne ilości wody. Ponadto, złożone zadania przetwarzania danych będzie można wykonać szybciej, zmniejszając czas działania serwerów, a w konsekwencji ich zapotrzebowanie na energię i chłodzenie.

6.3 PIOTR KOWALSKI

MANAGING DIRECTOR, PLDCA

Braki energii na rynkach europejskich są widoczne. Jak Stowarzyszenie PLDCA adresuje ten temat na rodzimym rynku? Jakie kroki podejmują Państwo w celu redukcji zużycia energii w centrach danych?

Dostęp do energii elektrycznej stał się jednym z najważniejszych czynników warunkujących wzrost sektora centrów przetwarzania danych, szczególnie w kontekście znaczącego skoku zapotrzebowania związanego z nowymi obiektami dedykowanymi sztucznej inteligencji. Tak zwane fabryki sztucznej inteligencji (ang. AI-Factories) liczone są w setkach megawat mocy przyłączeniowej, pojawiły się nawet ogłoszenia prasowe Google i QTS o projektach

przekraczających 1GW (1000MW). Są miejsca, jak Irlandia, gdzie centra danych odpowiadają za blisko 20% całkowitego zapotrzebowania na energię kraju i zatrzymano wydawanie kolejnych pozwoleń na budowę, ze względu na ograniczenie wydajności sieci. Coraz popularniejsze stają się dyskusje o dedykowanej produkcji prądu dla kampusów data center, czy to w formie turbin gazowych – już stosowane rozwiązanie – jak i wprowadzenia nowatorskich rozwiązań jak SMR (małe reaktory jądrowe). Jako Stowarzyszenie firm z łańcucha wartości centrów danych, staramy się podnosić świadomość potrzeb branży na polskim rynku. Nawiązaliśmy współpracę zarówno z innymi stowarzyszeniami branż współpracujących z centrami danych – energetyczną i ciepłowniczą – jak również bezpośrednio z Polskimi Sieciami Elektroenergetycznymi, które w swoim planie rozwoju sieci wysokiego napięcia w Polsce, przewidują wzrost zapotrzebowania na centra danych do 1200MW w 2034r. Równie ważnym tematem poza dostępnością energii, jest również jej ślad węglowy – temat kluczowy przy wyborze lokalizacji dla nowych centrów danych dla globalnych operatorów chmury obliczeniowej i sztucznej inteligencji. W tym zakresie Polska ma jeszcze dużo do zrobienia, ale na szczęście jesteśmy obecnie w czołówce krajów inwestujących z odnawialne źródła energii – fotowoltaikę oraz farmy wiatrowe, zarówno on-shore jak i off-shore. Dla PLDCA, promowanie rozwiązań o niskiej emisji CO_2 jest jednym z kluczowych zadań, mających fundamentalny wpływ na wzrost branży.

Jak w Pana perspektywie branża Data Center zmieni się w ciągu kolejnych 3-4 lat?

Wkraczamy w erę sztucznej inteligencji. Jej podstawowe skutki to znaczący wzrost skali obiektów – liczonych już teraz w ułamkach gigawat – a także konieczności przystosowania data center do obsługi serwerów o ekstremalnie wysokich gęstościach ciepła. Najnowsza specyfikacja szaf serwerowych na potrzeby sztucznej inteligencji (Nvidia NVL72) to aż 132kW prądu i ciepła na rack, a już dziś mówi się o konfiguracjach sięgających 250kW lub nawet 1MW. To są wartości, w których jeszcze całkiem niedawno liczyło się wielkość całych obiektów przeznaczonych do przetwarzania danych. Wymaga to zmiany paradygmatu projektowania oraz zupełnie nowych rozwiązań technologicznych zarówno po stronie zasilania, jak i chłodzenia serwerów. Szturmem na rynek wdzierają się systemy chłodzenia serwerów cieczą, dwie dominujące technologie – bezpośrednie chłodzenie procesorów (ang. direct-to-chip) oraz chłodzenie zanurzeniowe (ang. immersion cooling). Rosnąca gęstość ciepła zmienia również układ architektoniczny obiektów, z rosnącym udziałem przestrzeni dedykowanej na potrzeby urządzeń zasilania podstawowego i rezerwowego oraz przestrzeni potrzebnej do odprowadzania ciepła, w porównaniu z przestrzenią do przetwarzania danych (ang. White Space). Nadchodzące lata obfitować będą w innowacje technologiczne i projektowe, więc będzie to z pewnością bardzo ciekawy okres, w porównaniu z ostatnimi laty względnej stabilizacji rozwiązań przeznaczonych na potrzeby chmury obliczeniowej.

Boom na AI zaskoczył wszystkich, także operatorów Data Center. Co może wpłynąć równie silnie na podaż centrów danych po AI?

Nikt nie potrafi sobie dziś wyobrazić, co nastąpi „po AI" - a to z tej prostej przyczyny, że nie potrafimy jeszcze nawet do końca określić skali infrastruktury potrzebnej do wdrożenia sztucznej inteligencji. Mówi się teraz o dublowaniu zapotrzebowania na globalną moc centrów danych co 4-5lat oraz konieczności globalnych inwestycji na poziomie 1,5biliona dolarów w ciągu najbliższych pięciu lat. Dla porównania, to około dwukrotność PKB Polski w 2023r. Słyszałem nawet opinie, że rynek data center dla AI jest dziś tam, gdzie rynek przeznaczony chmurze obliczeniowej był w 2009r. Może to oznaczać, że na naszych oczach rodzi się największy przemysł XXI. wieku – nie przez przypadek pojawienie się rozwiązań sztucznej inteligencji nazywane jest przez wielu IV. rewolucją przemysłową. Obiekty tej skali należy już traktować w kontekście infrastrukturalnym i konieczne jest wiele lat, aby wybudować zarówno centra danych, jak i infrastrukturę energetyczną konieczną do zaspokojenia tego popytu.

Jakie trendy ekologiczne w branży data center uważa Pan za najważniejsze w najbliższych latach?

Bez wątpienia najważniejszym trendem w branży centrów danych jest dążenie do neutralności klimatycznej (Net Zero), do której zobowiązały się największe globalne firmy technologiczne jak Amazon Web Services, Google czy Microsoft. Firmy te, a co tym idzie cała branża intensywnie poszukuje rozwiązań pozwalających na redukcję śladu węglowego. Standardem stało się zasilenia obiektów w 100% zieloną energią, czy to na podstawie certyfikatów pochodzenia (PPA), czy też bezpośredniego zasilania obiektów ze źródeł odnawialnych. Bardzo dużo pracy wkłada się w poszukiwanie skutecznego modelu odzysku ciepła będącego ubocznym produktem przetwarzania danych. Rozważa się szereg zastosowań – rolnictwo wertykalne, hodowlę larw mącznika (lub innych wysokobiałkowych źródeł pokarmu dla ludzi

i zwierząt), czy też odzysk ciepła na potrzeby hodowli zwierząt, np. farmy krewetek lub łososi. Ze względu jednak na obecną i przyszłą skalę obiektów centrów danych, najbardziej obiecujący wydaje się kierunek odzysku ciepła do miejskiej sieci ciepłowniczej i zasilenia obiektów mieszkalnych energią odpadową. Branża ciepłownicza również ma bardzo wysokie zobowiązania dekarbonizacyjne wynikające z polityki klimatycznej Unii Europejskiej opisanych w Dyrektywie Energetycznej EED, współpraca z centrami danych wydaje się więc tutaj być idealną konfiguracją. Jest to również szansa dla Polski, aby wyróżnić się na tle krajów członkowskich, ponieważ dysponujemy drugą największą siecią ciepłowniczą w Europie i już dziś moglibyśmy zacząć wykorzystywać rozwiązania odzysku ciepła z centrów danych. Jako Stowarzyszenie PLDCA nawiązaliśmy współpracę z branżą ciepłowniczą oraz Ministerstwem Klimatu i Środowiska, aby pokazywać te możliwości i promować ich zastosowanie. Ostatnim elementem, który chciałbym wspomnieć, to ograniczenie wpływu na środowisko systemów zasilania rezerwowego - agregatów prądotwórczych – które dziś w większości napędzane są olejem napędowym (popularnym dieslem), ale ze względu na konieczność ograniczenia emisji zastępowane są paliwami alternatywnymi (HVO) lub – prawdopodobnie w przyszłości – wodorem. To obszar, który warto obserwować, bo zachodzą w nim dynamiczne zmiany.

Jakie są długoterminowe cele strategiczne Stowarzyszenia PLDCA?

Stowarzyszenie PLDCA ma trzy filary funkcjonowania. Po pierwsze, budowanie świadomości strategicznej wartości branży centrów danych dla rozwoju nowoczesnego państwa. Centra danych są na pierwszych stronach nowoczesnej polityki krajów wysoko rozwiniętych. Wielka Brytania ogłosiła niedawno obiekty przetwarzania danych jako kluczową część infrastruktury krytycznej kraju – na równi z systemem ochrony zdrowia – zapewniając dostęp do zasobów strategicznych kraju, ułatwione procedury administracyjne oraz bezpośrednio angażując się w pozyskiwanie inwestycji zagranicznych w tym sektorze. Analogiczne ruchy widzimy Stanach Zjednoczonych, Niemczech czy krajach skandynawskich. Drugim celem Stowarzyszenia jest promowanie Polski jako atrakcyjnego kraju dla inwestycji w centra przetwarzania danych – zarówno poprzez działania usuwające lokalne bariery rozwoju – współpracę z branżą energetyczną, ciepłowniczą oraz lokalnymi i krajowymi strukturami władzy - jak i poprzez współpracę z Europejskim Stowarzyszeniem Data Center (EUDCA) i uczestnictwo w międzynarodowych wydarzeniach branżowych. Trzecim celem jest integracja polskiej branży centrów danych – w całych łańcuchu wartości - od projektowania, przez realizację obiektów i ich późniejszą eksploatację. Zależy nam edukacji, wymianie najlepszych praktyk pomiędzy przedsiębiorstwami zrzeszonymi w PLDCA, pozyskiwaniu wykształconych kadr a także promowaniu najnowocześniejszych rozwiązań technologicznych, umożliwiających uzyskanie przewagi konkurencyjnej w międzynarodowym wyścigu o technologiczny popyt. Działania PLDCA zostały zauważone i docenione, co szczególnie widać po szybko rosnącej liczbie firm należących do Stowarzyszenia.

7. CASE STUDY CHMURA W KONTEKŚCIE DATA CENTER

7A. PRZYKŁADY WDROŻEŃ INNOWACYJNYCH ROZWIĄZAŃ

7.1 ORACLE DEDICATED REGION CLOUD@CUSTOMER – KOMPLETNA PRYWATNA CHMURA W TWOIM CENTRUM DANYCH

Jakub Madej

Technology Cloud Director Public & Enterprise

W erze cyfrowej, w której większość organizacji zaczyna coraz częściej korzystać z modeli chmurowych, globalni dostawcy usług oferują coraz bardziej elastyczne i bezpieczne rozwiązania. Oracle ogłaszając we wrześniu tego roku partnerstwo z AWS (takie partnerstwa był już wcześniej z Microsoft oraz Google) w zakresie wspólnego oferowania usług chmurowych umocnił się na pozycji lidera w kategorii multicloud. Warto także zwrócić uwagę na rozwiązanie, które zaczyna szczególnie zyskiwać na popularności - Dedicated Region Cloud@Customer – jest to propozycja od Oracle dla klientów potrzebujących prywatnej, w pełni funkcjonalnej chmury obliczeniowej w ramach własnego centrum danych. Oracle Dedicated Region Cloud@Customer pozwala przedsiębiorstwom i instytucjom korzystać z wszystkich dostępnych usług chmurowych bez konieczności migracji do publicznej chmury, co czyni ją idealnym rozwiązaniem dla organizacji o wysokich wymaganiach w zakresie rezydencji danych, bezpieczeństwa, prywatności i zgodności z regulacjami.

Czym jest DRCC - Oracle Dedicated Region Cloud@Customer?

Oracle Dedicated Region Cloud@Customer to tożsama paleta usług chmurowych jaką znajdziemy w ramach Oracle Cloud Infrastructure, dostarczana bezpośrednio do fizycznego centrum danych wskazanego przez klienta. Oznacza to, że wszystkie usługi i możliwości dostępne w publicznej chmurze Oracle – takie jak przetwarzanie i przechowywanie danych, analityka, sztuczna inteligencja, blockchain, itp., a także oprogramowanie ERP, EPM, HCM czy CX jako usługa (SaaS) – mogą być uruchamiane w prywatnym regionie chmurowym dostępnym wyłącznie dla jednej organizacji.
To rozwiązanie zapewnia identyczne API, przepływy pracy i zasady bezpieczeństwa jak publiczna chmura Oracle, umożliwiając organizacjom zachowanie pełnej kontroli nad swoimi danymi, jednocześnie oferując elastyczność i wydajność chmury.

Kluczowe Korzyści DRCC - Oracle Dedicated Region Cloud@Customer

1. Elastyczność Publicznej Chmury w Prywatnym Środowisku

Dedicated Region Cloud@Customer dostarcza wszystkie zalety publicznej chmury – skalowalność, automatyzację, dostęp do najnowszych technologii – w prywatnym, izolowanym środowisku klienta. Organizacje mogą dynamicznie skalować zasoby w zależności od potrzeb, jednocześnie gwarantując sobie wyłączność wykorzystywania dedykowanej infrastruktury. Oracle na bieżąco monitoruje jej wykorzystanie i z wyprzedzeniem dokonuje rozbudowy pod kątem dostosowania do rosnących potrzeb.

2. Zgodność z Regulacjami i Bezpieczeństwo

W niektórych sektorach, takich jak utilities, finanse, opieka zdrowotna czy administracja, regulacje prawne wymagają przechowywania danych w obrębie kraju lub w określonych lokalizacjach. Dedicated Region Cloud@Customer pozwala firmom na spełnianie tych wymagań bez jednoczesnej konieczności rezygnacji z zalet chmury publicznej. Ponadto, rozwiązanie to spełnia najwyższe standardy bezpieczeństwa, takie jak szyfrowanie danych w spoczynku i podczas przesyłania, zarządzanie kluczami szyfrowania, a także zgodność z międzynarodowymi certyfikatami bezpieczeństwa.

3. Minimalizacja Opóźnień

Dzięki fizycznemu umiejscowieniu Dedicated Region Cloud@Customer w siedzibie klienta, opóźnienia w dostępie do aplikacji i danych są znacząco minimalizowane. To szczególnie istotne w przypadku aplikacji, które wymagają niskich czasów reakcji, takich jak systemy transakcyjne czy aplikacje, gdzie czas odpowiedzi ma krytyczne znaczenie.

4. Pełna Integracja z Lokalną Infrastrukturą

Dedicated Region Cloud@Customer umożliwia łatwą integrację z istniejącą infrastrukturą IT, zarówno w zakresie sieci, jak i operacji. Oferowane są również zaawansowane funkcje zarządzania, które pozwalają na efektywne monitorowanie zasobów oraz procesów w ramach jednego środowiska.

5. Aktualizacje i Rozwój Technologiczny

Oracle zapewnia, że Dedicated Region Cloud@Customer jest regularnie aktualizowany o najnowsze poprawki, technologie i usługi dostępne w publicznej chmurze Oracle. Klienci mogą korzystać z najnowszych funkcji w obszarze sztucznej inteligencji, uczenia maszynowego, analityki danych i wielu innych technologii bez konieczności przenoszenia się do publicznej chmury.

Przykłady zastosowań

Dedicated Region Cloud@Customer sprawdza się w różnych sektorach a zwłaszcza tam, gdzie wysoki poziom bezpieczeństwa danych oraz niskie opóźnienia są kluczowe.

- Utilities: Firmy z sektora Energy,Oil&Gas mogą korzystać z Dedicated Region Cloud@Customer, aby w pełni kontrolować swoje dane i aplikacjami, gdzie nie bez znaczenia jest fakt, że odpowiadają za infrastrukturę krytyczną, przy

jednoczesnym wykorzystaniu najnowocześniejszej technologii chmurowej.

- Sektor Finansowy: Banki i inne instytucje finansowe mogą korzystać z Dedicated Region Cloud@Customer do obsługi krytycznych aplikacji, przetwarzania transakcji oraz analizy danych, jednocześnie zapewniając zgodność z regulacjami prawnymi dotyczącymi prywatności i bezpieczeństwa danych. Fakt przechowywania i przetwarzania danych w lokalizacji klienta a także ściśle określone mechanizmy aktualizacji i najwyższe standardy bezpieczeństwa w znaczący sposób ułatwiają spełnienie regulacji jakim podlegają podmioty nadzorowane (Prawo Bankowe, Komunikat Chmurowy KNF, NIS2 czy DORA).

- Opieka Zdrowotna: Organizacje z sektora ochrony zdrowia mogą przechowywać i analizować dane pacjentów w prywatnym środowisku chmurowym, spełniając jednocześnie standardy zgodności z przepisami takimi jak HIPAA.

- Administracja Publiczna: Organy rządowe mogą korzystać z Dedicated Region Cloud@Customer, aby utrzymywać pełną kontrolę nad swoimi danymi i aplikacjami w obrębie własnych granic, jednocześnie korzystając z nowoczesnych technologii chmurowych.

Podsumowanie

Dedicated Region Cloud@Customer to jedyne na rynku rozwiązanie, które pozwala organizacjom korzystać z pełnej mocy i wszystkich usług chmury publicznej, zachowując jednocześnie kontrolę nad danymi i wyłącznym dostępem do infrastruktury znajdującej się w prywatnym środowisku. Dzięki temu modelowi firmy i instytucje mogą czerpać korzyści z najnowszych technologii chmurowych, jednocześnie spełniając rygorystyczne wymagania dotyczące bezpieczeństwa i zgodności z regulacjami. Dla wielu klientów Dedicated Region Cloud@Customer stanowi odpowiedź na wyzwania współczesnej transformacji cyfrowej, zapewniając elastyczność, bezpieczeństwo oraz zgodność w jednym pakiecie.

7.2 CENTRALNY OŚRODEK INFORMATYKI, MINISTERSTWO CYFRYZACJI, NASK PIB

Andrzej Tokarzewski
Architekt - Zespół Polityk, Strategii i Rozwoju Chmury, COI

Ministerstwo Cyfryzacji (MC) we współpracy z Centralnym Ośrodkiem Informatyki (COI).

- MC - Administracja rządowa, cyfryzacja, COI - Technologie informacyjne, sektor publiczny

- **Misją MC** jest dążenie aby Polska była państwem innowacyjnym i przyjaznym, w którym interakcje między państwem, obywatelami i przedsiębiorcami są proste i efektywne poprzez skuteczną cyfryzację. Natomiast misją **COI** jest realizacja projektów IT dla sektora publicznego, dostarczając nowoczesnych usług i narzędzi, które przyczyniają się do cyfrowej transformacji kraju.

- **Wartości** reprezentowane przez **MC** to dążenie do poprawy jakości życia obywateli poprzez cyfryzację usług publicznych, dotrzymywanie słowa, budowanie standardów, szacunek dla pieniędzy publicznych. Natomiast **COI** reprezentuje innowacyjność, kreatywność, zaangażowanie, dążenie do bycia liderem cyfryzacji w Europie i na świecie.

Administracja publiczna borykała się z wieloma wyzwaniami związanymi z zarządzaniem danymi i infrastrukturą IT. Tradycyjne systemy były często przestarzałe, kosztowne w utrzymaniu i nieefektywne. Problemy te obejmowały:

- **Brak skalowalności:**
Tradycyjne systemy IT (rozwiązania silosowe) nie były w stanie szybko dostosowywać się do zmiennych potrzeb administracji;

- **Wysokie koszty:** Utrzymanie i modernizacja infrastruktury IT wiązały się z dużymi wydatkami;

- **Bezpieczeństwo danych:**
Rosnące zagrożenia cybernetyczne wymagały bardziej zaawansowanych rozwiązań w zakresie ochrony danych;

- **Efektywność operacyjna:**
Przestarzałe systemy często prowadziły do opóźnień i nieefektywności w realizacji zadań administracyjnych.

Dlatego administracja publiczna zdecydowała się na wdrożenie **chmury rządowej** w modelu społecznościowym w ramach Wspólnej Infrastruktury Informatycznej Państwa **(projekt WIIP)**, aby sprostać powyższym wyzwaniom i wykorzystać nowe możliwości technologiczne. Kluczowe powody to:

- centralizacja przetwarzania istotnych danych i systemów IT;
- zwiększenie elastyczności poprzez szybkie skalowanie zasobów w zależności od potrzeb;
- poprawa bezpieczeństwa poprzez stosowanie ustandaryzowanych zaawansowanych mechanizmów ochrony danych;
- zwiększenie efektywności poprzez automatyzację i lepsze zarządzanie danymi.
- standaryzacja wytwarzania systemów IT;
- zapewnienie obywatelom wydajniejszych i bardziej niezawodnych e-usług;

Chmura pozwala na zmodernizowanie i usprawnienie zarządzania danymi oraz infrastrukturą IT. Jest to zaawansowane rozwiązanie technologiczne, które umożliwia przechowywanie, przetwarzanie i udostępnianie danych w sposób bardziej efektywny i bezpieczny.

Wdrożenie chmury rządowej przyniosło szereg korzyści dla administracji publicznej, w tym:

- przyspieszenie realizacji zadań administracyjnych poprzez automatyzację procesów i lepsze zarządzanie danymi;
- optymalizację kosztów poprzez zmniejszenie wydatków na infrastrukturę IT i zwiększenie efektywności operacyjnej;
- wsparcie innowacji umożliwiające szybkie wdrażanie nowych technologii i rozwiązań IT.
- poprawę bezpieczeństwa danych;
- skalowalność;
- dostępność i niezawodność zapewniające ciągłość działania administracji publicznej;
- systematyczną likwidację długu technologicznego.

Proces wdrożenia chmury rządowej obejmował kilka kluczowych kroków:

- analiza potrzeb na podstawie inwentaryzacji obecnej infrastruktury IT i identyfikacji obszarów wymagających modernizacji. Opracowanie strategii wdrożenia chmury, uwzględniającej cele i wymagania administracji publicznej;
- wybór dostawcy rozwiązań IT gwarantujący spełnienie wymagań bezpieczeństwa i jakości;
- konfiguracja chmury i wdrożenia procesów;
- migracja systemów oraz testowanie i weryfikacja poprawności migracji;
- szkolenie pracowników w zakresie korzystania z nowych narzędzi i usług chmurowych;
- monitorowanie i optymalizacja działania chmury i jej wykorzystania. Rozbudowa potencjału chmury rządowej i projektowanie nowych usług typu IaaS, PaaS i SaaS.

Realizacja projektu wdrożenia chmury rządowej trwała 36 miesięcy.

Cele wdrożenia chmury zostały w dużej mierze zrealizowane w obszarze poprawy jakości usług, bezpieczeństwa danych oraz optymalizacji kosztów.

Z wdrożenia chmury rządowej administracja publiczna wyciągnęła kilka kluczowych lekcji dotyczących znaczenia planowania, konieczności ciągłej adaptacji technologicznej oraz współpracy w obszarze standaryzacji infrastruktury IT.

Administracja publiczna planuje kontynuować wdrażanie innowacji technologicznych. Plany te obejmują rozwój usług cyfrowych, integrację nowych technologii oraz zwiększanie bezpieczeństwa.

7B. CASE STUDY DOTYCZĄCE WYZWAŃ ORAZ ROZWIĄZAŃ ZAPROPONOWANYCH PRZEZ FIRMY

7.1. CENTRALNY OŚRODEK INFORMATYKI, MINISTERSTWO CYFRYZACJI, NASK PIB

Andrzej Tokarzewski

Architekt - Zespół Polityk, Strategii i Rozwoju Chmury, COI

Ministerstwo Cyfryzacji **(MC)** we współpracy z Naukową i Akademicką Siecią Komputerową Państwowy Instytut Badawczy **(NASK PIB)** oraz Centralnym Ośrodkiem Informatyki **(COI).**

- MC - Administracja rządowa, cyfryzacja, COI - Technologie informacyjne, sektor publiczny, NASK PIB – cyberbezpieczeństwo, technologie informacyjne.

- Misją MC jest dążenie aby Polska była państwem innowacyjnym i przyjaznym, w którym interakcje między państwem, obywatelami i przedsiębiorcami są proste i efektywne poprzez skuteczną cyfryzację. Misją NASK PIB jest zapewnienie bezpieczeństwa cybernetycznego oraz ochrona użytkowników internetu. Instytut działa na rzecz rozwoju technologii informacyjnych i komunikacyjnych, wspierając zarówno sektor publiczny, jak i prywatny. Natomiast misją COI jest realizacja projektów IT dla sektora publicznego, dostarczając nowoczesnych usług i narzędzi, które przyczyniają się do cyfrowej transformacji kraju.

- Wartości reprezentowane przez MC to dążenie do poprawy jakości życia obywateli poprzez cyfryzację usług publicznych, dotrzymywanie słowa, budowanie standardów, szacunek dla pieniędzy publicznych. NASK dąży do odpowiedzialnego zarządzania technologiami i zasobami, efektywnego wdrażania innowacyjnych rozwiązań oraz promowania otwartości na nowe idee i technologie. Natomiast COI reprezentuje innowacyjność, kreatywność, zaangażowanie, dążenie do bycia liderem cyfryzacji w Europie i na świecie.

2. MC stanęło przed koniecznością modernizacji infrastruktury przetwarzania danych, aby zapewnić ciągłość, bezpieczeństwo i integralność zasobów administracji publicznej. Istniejące centra danych (CPD) i serwerownie są w dużej liczbie przestarzałe i nieefektywne energetycznie, co stwarza ryzyko dla bezpieczeństwa systemów informatycznych, integralności danych w nich przetwarzanych oraz stabilności usług publicznych.

MC chciało osiągnąć następujące cele:

- zwiększenie bezpieczeństwa danych i systemów administracji publicznej;

- poprawę efektywności energetycznej infrastruktury IT;

- zapewnienie ciągłości świadczenia usług publicznych **(e-usług),** nawet w sytuacjach kryzysowych a w konsekwencji zapewnienia ciągłości działania państwa.

3. MC zdecydowało się na budowę trzech nowoczesnych, ustandaryzowanych i efektywnych energetycznie CPD, zgodnych z normą PN-EN 50600 w ramach projektu Krajowe Centra Przetwarzania Danych **(KCPD).** CPD te mają wykorzystywać odnawialne źródła energii, co przyczyni się do zmniejszenia śladu węglowego. Budowa KCPD jest inwestycją strategiczną, która istotnie wpłynie na zapewnienie ciągłości działania systemów IT o krytycznym znaczeniu dla Państwa, np. działanie rejestrów państwowych i chmury rządowej **(RChO),** które stanowią bazę do świadczenia e-usług niezbędnych dla stabilnego funkcjonowania społeczeństwa i administracji państwowej w życiu codziennym i w sytuacjach kryzysowych. Ponadto, dostarczy dalszych ułatwień dla „obywatela cyfrowego" oraz podniesie bezpieczeństwo i integralność danych tam przetwarzanych. Budowa KCPD realizuje założenia Inicjatywy Wspólnej Infrastruktury Informatycznej Państwa **(WIIP).**

Proces wdrożenia KCPD obejmuje kilka kluczowych kroków:

- przygotowanie projektu - wybór biura projektowego, inżyniera kontraktu oraz

generalnego wykonawcy;

- budowa - realizacja budowy trzech CPD;
- testowanie i uruchomienie - przeprowadzenie testów i uruchomienie CPD;
- monitorowanie i optymalizacja - ciągłe monitorowanie działania CPD i wprowadzanie optymalizacji;
- migracja systemów informatycznych z istniejących centrów i serwerowni do KCPD. Ten etap jest poza budżetem projektu KCPD.

Harmonogram realizacji projektu obejmuje okres od 1 września 2023 r. do 31 marca 2025 r., a całkowity koszt inwestycji wynosi prawie 830 mln zł.

Dzięki wdrożeniu KCPD, administracja publiczna osiągnie znaczące rezultaty:

- zwiększenie bezpieczeństwa danych - nowoczesne CPD zapewniają wyższy poziom ochrony przed cyberatakami i awariami;
- poprawa efektywności energetycznej - wykorzystanie odnawialnych źródeł energii i nowoczesnych technologii pozwoli na zmniejszenie zużycia energii;
- zapewnienie ciągłości usług - nowa infrastruktura IT gwarantuje nieprzerwane działanie kluczowych systemów administracji publicznej, nawet w sytuacjach kryzysowych;
- większa niezawodność - użytkownicy e-usług mogą liczyć na stabilność, bezpieczeństwo i integralność danych;
- oszczędności energetyczne - zmniejszenie kosztów operacyjnych dzięki efektywniejszemu wykorzystaniu energii;
- lepsza ochrona - wyższy poziom zabezpieczeń przed cyberzagrożeniami.

6. Cele wdrożenia KCPD w dużej mierze zrealizowane w obszarze poprawy jakości usług, bezpieczeństwa danych oraz optymalizacji kosztów.
Lekcje wyciągnięte z przygotowania projektu KCPD to dokładne planowanie i analiza ryzyka oraz efektywna współpraca między różnymi jednostkami administracji publicznej i partnerami zewnętrznymi. To podnosi szansę na skuteczną realizację skomplikowanych przedsięwzięć.

Administracja publiczna planuje kontynuować wdrażanie innowacji technologicznych. Plany obejmują dalszy rozwój infrastruktury IT, w tym rozbudowę RChO o kolejne usługi chmurowe i wdrażanie nowych rozwiązań technologicznych.

7.2 SEDIVIO SA

Olga Budziszewska

Cybersecurity Strategy and Compliance Advisor w SEDIVIO

Wyzwanie

Organizacja finansowa postanowiła wdrożyć aplikację do obsługi klientów korporacyjnych w sektorze ubezpieczeń, opartą na publicznej chmurze obliczeniowej. Ze względu na przetwarzanie danych wrażliwych, pojawiły się wyzwania związane z regulacjami prawnymi i wymaganiami bezpieczeństwa. Podczas prezentacji wczesnej wersji produktu firma odkryła braki w wymaganiach bezpieczeństwa, które uniemożliwiały uruchomienie usługi.
Z uwagi na napięty harmonogram (wynikający z późnego etapu, na którym zidentyfikowano wymagania regulacyjne oraz bezpieczeństwa), organizacja zdecydowała się na wykorzystanie rozwiązania Cyrima.

- **Dlaczego firma zdecydowała się na wdrożenie Cyrimy?**

Wdrożenie aplikacji chmurowej w sektorze finansowym to złożony proces, wymagający współpracy wielu działów (biznes, IT, prawo, bezpieczeństwo, ryzyko, audyt). Koordynacja działań pomiędzy tymi obszarami jest kluczowa. Brak uwzględnienia wymagań regulacyjnych i bezpieczeństwa na wczesnych etapach groził opóźnieniami i przekroczeniem budżetu. Organizacja zdecydowała się na wdrożenie Cyrimy z kilku powodów.

- Aplikacja umożliwiła szybkie uzyskanie pełnego backlogu zadań związanych ze zgodnością i bezpieczeństwem, eliminując potrzebę dodatkowych konsultantów.
- Wymogi sektora finansowego i związane z nimi ryzyka wymagały kompleksowego rozwiązania do identyfikacji i wdrożenia wymagań bezpieczeństwa, aby uniknąć zablokowania usługi w fazie produkcyjnej.
- Instrukcje dostępne w Jirze pozwoliły na kontynuację prac developerskich bez opóźnień.
- Ograniczony budżet uniemożliwiał zatrudnienie konsultantów bezpieczeństwa na pełen etat. Cyrima umożliwiła wewnętrznemu zespołowi realizację zadań, korzystając z konsultantów tylko w kluczowych momentach.

Cele, jakie firma chciała osiągnąć poprzez wprowadzenie rozwiązania

Głównym celem było zapewnienie wsparcia zespołom wdrożeniowym w obszarze identyfikacji oraz wdrożenia odpowiednich działań zapewniających realizację wymagań regulacyjnych oraz bezpieczeństwa organizacji.

Opis rozwiązania Cyrima

Cyrima to nowatorskie rozwiązanie wspierające bezpieczeństwo i zgodność regulacyjną w zarządzaniu projektami. Składa się z trzech modułów: frameworku, silnika zarządzania wiedzą (plugin) oraz marketplace'u. Framework, główny komponent Cyrimy, oferuje procesy, standardy oraz instrukcje stanowiskowe (zadania w Jira). Dzięki parametryzacji pod kątem cech organizacji (skala, lokalizacja, branża) i cech projektu (rodzaj, skala, ryzyko), zespoły mogą szybko otrzymać kompletny backlog zadań w Jira, niezbędnych do realizacji projektów zgodnie z wymogami bezpieczeństwa i regulacji.

Proces wdrożenia rozwiązania (kroki, zaangażowane zasoby, harmonogram)

Wdrożenie Cyrimy w organizacji na potrzeby opisywanego projektu odbyło się podczas dwóch sesji warsztatowych z zespołem wdrożeniowym, przedstawicielem linii biznesowej oraz reprezentantami działów bezpieczeństwa i zgodności. Dodatkowo, w ramach realizacji zadań projektowych, konsultanci Cyrimy wspierali prace projektowe w niezbędnym, ściśle określonym zakresie.

Jakie korzyści przynosi to rozwiązanie dla firmy i jej klientów

Wykorzystanie Cyrimy w procesach wytwórczych i wdrożeniowych pozwala na optymalne zaadresowanie wymagań regulacyjnych i bezpieczeństwa zgodnie z profilem organizacji i realizowanym projektem. Dzięki integracji z Jira, zespoły projektowe otrzymują pełen zakres zadań dotyczących zgodności i bezpieczeństwa, co umożliwia precyzyjne planowanie budżetu, harmonogramu i zasobów. Ponadto, dzięki Cyrimie organizacja zyskuje:

- szybki dostęp do wiedzy na temat wymagań regulacyjnych i bezpieczeństwa, eliminując potrzebę czasochłonnych analiz;
- klarowne instrukcje stanowiskowe, umożliwiające zespołom wdrożeniowym samodzielne realizowanie zadań bez angażowania specjalistów od bezpieczeństwa; zwiększenie efektywności pracy zespołów wdrożeniowych, skrócenie czasu oraz zmniejszenie budżetu potrzebnego do uruchomienia usługi lub wprowadzenia produktu na rynek - struktura Frameworku zaprojektowana tak, aby uniknąć kosztownych poprawek wynikających z braku synchronizacji z wymogami bezpieczeństwa.

8. KOMENTARZE DO RAPORTU

Fundusze Europejskie na rozwój innowacyjnych przedsiębiorstw

Każdy przedsiębiorca, który ma pomysł na innowację – nowy produkt, technologię, usługę czy proces może zgłosić się po środki z Funduszy Europejskich, którymi dysponuje Narodowego Centrum Badań i Rozwoju (NCBR). W branży centrów danych jest sporo przestrzeni na innowacje, a zastosowanie rozwiązań cyfrowych czy chmurowych wykładniczo rośnie na całym świecie, co dodatkowo daje szerokie możliwości rozwoju segmentu.

Narodowe Centrum Badań i Rozwoju jako agencja rządowa łącząca świat nauki i biznesu, tworzy odpowiednie warunki do prowadzenia prac badawczo-rozwojowych. Poprzez współfinansowanie procesów B+R wspiera rodzimych przedsiębiorców, istotnie zmniejszając ich ryzyko biznesowe towarzyszące wdrażaniu przełomowych projektów badawczych. Misją NCBR jest realizacja zadań służących społecznemu i gospodarczemu rozwojowi Polski oraz rozwiązywanie konkretnych cywilizacyjnych problemów jej mieszkańców. Przez 17 lat działalności Centrum wsparło kilkanaście tysięcy projektów kwotą blisko 80 miliardów złotych.

NCBR jest Instytucją Pośredniczącą w programie Fundusze Europejskie dla Nowoczesnej Gospodarki (FENG) na lata 2021-2027. Jest to największy krajowy program wspierania innowacyjności. Za jego pośrednictwem do polskich firm trafi łącznie 7,9 mld euro. FENG jest w dużej mierze kontynuacją Programu Inteligentny Rozwój, ale cechuje się nowym, kompleksowym podejściem do potrzeb przedsiębiorcy dotyczących prowadzenia prac badawczo-rozwojowych i wdrożenia ich wyników. Wdrażane projekty mają wzmocnić polską gospodarkę i przestawić ją na jeszcze wyższy poziom zaawansowania technologicznego i proekologicznego. Łączna kwota na wszystkie działania realizowane przez NCBR w ramach FENG wynosi 2,5 mld euro, czyli około 12 miliardów złotych.

Budżet Centrum stanowi więc ponad 30% całego budżetu programu.

Kompleksowe wsparcie

Ofertę największego konkursu w ramach programu FENG – Ścieżki SMART – w zależności od naboru NCBR kieruje do dużych firm, ich konsorcjów wraz z MŚP, organizacjami badawczymi lub organizacjami pozarządowymi oraz konsorcjów MŚP i organizacji badawczych lub organizacji pozarządowych. W konkursie nie ma ograniczeń tematycznych, ale każdy zgłoszony projekt musi wpisywać się w przynajmniej jedną Krajową Inteligentną Specjalizację. Modułowa formuła w konkursie sprawia, że Ścieżka SMART jest szyta na miarę zróżnicowanych potrzeb przedsiębiorców. Moduły dzielą się na obowiązkowe i fakultatywne. Konkurs gwarantuje więc kompleksowe, elastyczne i indywidualne podejście do prowadzenia prac B+R oraz wdrożenia ich wyników. W przypadku wsparcia, którego udziela NCBR, wniosek o dofinansowanie musi obejmować moduł B+R, który ma na celu doprowadzenie do opracowania innowacji produktowej lub innowacji w procesie biznesowym.

Każdy przedsiębiorca może również wybrać dodatkowy moduł lub kilka modułów rozszerzających projekt:

- moduł wdrożenie innowacji (czyli dofinansowanie na wdrożenie wypracowanej innowacji w formie produktów lub procesów biznesowych w zakresie produkcji wyrobów lub usług),
- moduł infrastruktura B+R - dofinansowanie na infrastrukturę niezbędną do tworzenia innowacji), moduł cyfryzacja (inwestycje związane zastosowaniem rozwiązań cyfrowych w przedsiębiorstwie zmierzających do cyfryzacji produkcji, procesów, jak i produktów, usług, modelu biznesowego oraz zapewnienia cyberbezpieczeństwa,
- moduł zazielenienie przedsiębiorstw - transformacja przedsiębiorstwa w kierunku zrównoważonego rozwoju oraz gospodarki w obiegu zamkniętym), moduł internacjonalizacja (promocja zagraniczna produktów - wyrobów lub usług lub uzyskanie ochrony praw własności przemysłowej oraz ich obronę w przypadku naruszenia,
- moduł kompetencje - doskonalenie i zdobywanie kwalifikacji, umiejętności oraz wiedzy zespołu projektowego.

Do 24 października 2024 roku trwa nabór w konkursie „Ścieżka SMART", skierowany do dużych przedsiębiorstw, z budżetem 890 mln zł. Jednakże, w tym roku Narodowe Centrum Badań i Rozwoju zaplanowało uruchomienie naboru Ścieżki SMART dla konsorcjów. Te będą mogły ubiegać się o łącznie 1,3 miliarda złotych dofinansowania. Ogłoszenie konkursu zaplanowane jest na 8 listopada 2024 roku, a nabór wniosków w terminie 10 stycznia – 28 marca 2025 roku.

8B. POLSKA CHMURA

Wiesław Wilk

Wiceprezes Zarządu Polcom,
Przewodniczący Związku Polska Chmura

Chmura „made in Poland" - bezpieczeństwo, suwerenność i innowacje

W dobie dynamicznych zmian w gospodarce, monitorowanie trendów i innowacji technologicznych powinno stanowić kluczowy element strategii każdej organizacji. Niemniej, niezależnie od trendów, warto mieć na uwadze uniwersalne i ponadczasowe wartości, które powinny stanowić fundament działalności każdej firmy, która bierze odpowiedzialność za przetwarzanie danych, takie jak ich bezpieczeństwo i suwerenność. Jako przedstawiciel Polskiej Chmury - związku polskich data center - pragnę zwrócić na nie uwagę. Uważamy bowiem, że tylko solidne fundamenty, zgodne z polską i europejską literą prawa, mogą da-

wać organizacjom przestrzeń na podążaniem za trendami.

Jurysdykcja i suwerenność danych

W istniejącym od ponad 8 lat związku Polska Chmura zebrały się we wspólnym głosie polskie centra danych, które od lat wspierają cyfrową transformację kraju i budują świadomość wokół suwerenności danych. Nasze organizacje specjalizują się w dostarczaniu bezpiecznych i nowoczesnych rozwiązań, które nie tylko niczym nie ustępują ofercie globalnych dostawców, a dodatkowo wyróżniają się atrakcyjną ceną, elastycznością dostosowywania do konkretnych projektów biznesowych oraz partnerskim podejściem na każdym etapie współpracy.

W kontekście rosnącej globalizacji i powszechnej dostępności usług chmurowych, chcemy zwrócić szczególną uwagę na problematykę związaną z jurysdykcją i suwerennością danych. Zgodnie z wieloma aktami prawnymi takimi jak, art. 3 ustawy o ochronie danych osobowych z dnia 10 maja 2018 r., przepisami ustawy o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 r.,rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa (tzw. Cybersecurity Act), **dane obywateli Polski, zwłaszcza te przetwarzane w systemach kluczowych dla bezpieczeństwa państwa, powinny być przetwarzane w sposób gwarantujący ich ochronę i zgodność z krajowym oraz unijnym prawem.** Warto wiedzieć, że transfer i przechowywanie danych poza granicami kraju, szczególnie poza jurysdykcją Unii Europejskiej, stanowi poważne zagrożenie dla bezpieczeństwa oraz suwerenności danych, zwiększając ryzyko nieautoryzowanego dostępu, modyfikacji lub niewłaściwego wykorzystania danych.

Zaawansowane technologie i współpraca

Dzięki zastosowaniu nowoczesnych technologii oraz kompetencjom rodzimych specjalistów, polskie centra danych efektywnie zarządzają ogromnymi wolumenami danych, zapewniając jednocześnie najwyższy poziom bezpieczeństwa. Doskonały przykład stanowią superkomputery, którymi dysponują należące do Polskiej Chmury Wrocławskie Centrum Sieciowo-Superkomputerowe (WCSS) oraz Akademickie Centrum Komputerowe Cyfronet AGH w Krakowie, które znajdują się w czołówce listy TOP500 najszybszych superkomputerów na świecie.

Te zaawansowane jednostki obliczeniowe stanowią kręgosłup technologiczny nie tylko dla projektów badawczych, ale także dla zaawansowanych rozwiązań komercyjnych. Polskie centra danych systematycznie inwestują w rozwój technologii, m.in. w zakresie sztucznej inteligencji (AI), co pozwala na tworzenie nowoczesnych, złożonych rozwiązań spełniających wymagania zarówno lokalnego, jak i globalnego rynku. Innowacje te są integralnym elementem strategii rozwoju polskich centrów danych, co pozwala na ciągłe podnoszenie jakości świadczonych usług.

Firmy zrzeszone w Polskiej Chmurze znajdują się w różnych częściach kraju. Charakteryzują się gotowością wzajemnej współpracy i oferowanie rozwiązań, które wykraczają poza możliwości jednego centrum danych. Oznacza to ogromny potencjał i gotowość do działania przy najtrudniejszych i największych projektach. O tej gotowości świadczą prowadzone przez związek projekty wspólne, m.in. PCH-X, czyli pierwsza sieć internetowa pomiędzy centrami danych w Polsce. Celem projektu jest zwiększenie bezpieczeństwa komunikacji i suwerenności danych. Projekt wymiany ruchu internetowego PCH-X połączył siecią firmy należące do Polskiej Chmury

Chmura „Made in Poland" i standardy bezpieczeństwa
Polskie centra danych są w pełni zgodne ze standardami takimi jak: NIS2, DORA, ISO 27001, ISO 27017, ISO 22301, ISO 9001, ISO 20000-1, NORM PN EN 1047-2, EN 50600, AQAP 2110, ANSI/TIA-942. Certyfikaty te potwierdzają, że spełniają one najwyższe normy w zakresie bezpieczeństwa informacji, ciągłości działania oraz zarządzania jakością. Oznacza to, że zarówno administracja rządowa, jak i firmy mogą z pełnym zaufaniem korzystać z usług polskich dostawców, mając pewność, że ich dane są przetwarzane zgodnie z najwyższymi standardami bezpieczeństwa

oraz pod nadzorem europejskiej jurysdykcji.

Warto również pamiętać, że współpraca z polskimi centrami danych przekłada się na dodatkowe korzyści w wymiarze makroekonomicznym, takie jak tworzenie lokalnych miejsc pracy oraz wspieranie gospodarki poprzez odprowadzanie podatków do krajowego budżetu.

W dobie powszechnej dostępności oraz walki zagranicznych podmiotów o polski rynek, warto pamiętać, że polskie centra danych oferują zaawansowane technologicznie rozwiązania, zgodne z europejskimi i międzynarodowymi standardami bezpieczeństwa. Jako przedstawiciele tego sektora, podkreślamy, że bezpieczeństwo danych oraz poszanowanie jurysdykcji powinny być priorytetem każdej firmy działającej w branży IT. Niezależnie od trendów, dane polskich obywateli powinny być przetwarzane w sposób bezpieczny, zgodny z obowiązującymi przepisami, przy wykorzystaniu najnowocześniejszych technologii. Jeśli dodatkowo wybór polskiego dostawcy wspiera polską gospodarkę oraz rynek pracy to jest to sytuacja win-win dla każdej ze stron.

8C. S4TECH

Jacek Kłonica **Krzysztof Piotrowski**
Michał Kandziora

S4Tech

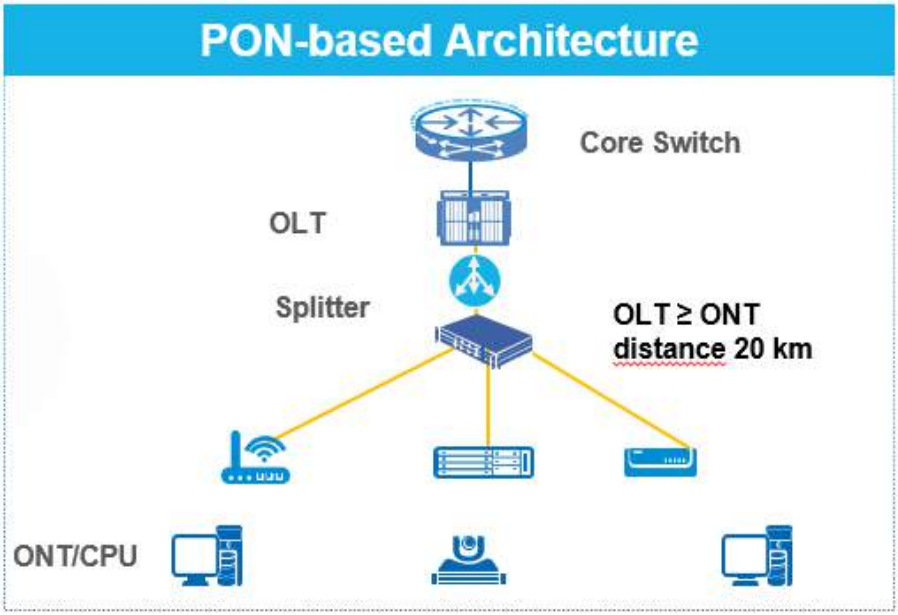
Rozwój zastosowań AI motorem technologicznych zmian w lokalnych (LAN)i metropolitalnych (MAN) sieciach transmisji danych

Rozwój aplikacji i usług opartych o sztuczną inteligencję (AI) w sposób znaczący wpłynie na zmiany w szerokopasmowych sieciach komunikacyjnych, wygeneruje zapotrzebowanie transmisji Zetabajtów (ZB) danych, które będą przetwarzane w infrastrukturze typu „cloud" – czyli rozproszonych Data Center. AI jest ogromnym wyzwaniem dla Data Center oraz dla systemów komunikacyjnych zarówno na poziomie sieci LAN (Local Area Network), dostępowych MAN (Metro Area Network) jak i w sieciach szkieletowych (WAN).

Istniejące sieci komunikacyjne będą musiały wkrótce sprostać nowym wymaganiom wynikającym z nieustannego przyrostu przetwarzanych danych: od 147 ZB (2024) do 291 ZB (2027)[1]. Istniejące systemy sieciowe muszą w związku z tym zostać rozbudowane do wydajności umożliwiających szkolenie dużych modeli językowych opartych na algorytmach uczenia się (LLM) i obsłudze aplikacji opartych na AI[2]. Sposobem na zapewnienie sprawnego przetwarzania zbiorów danych i zapewnienia żeby ich wymiana dokonywała się bez opóźnień będą zaawansowane i zarządzane przez aplikacje oparte na AI systemy sieciowe oraz gotowe na duże przepływności sieci światłowodowe.

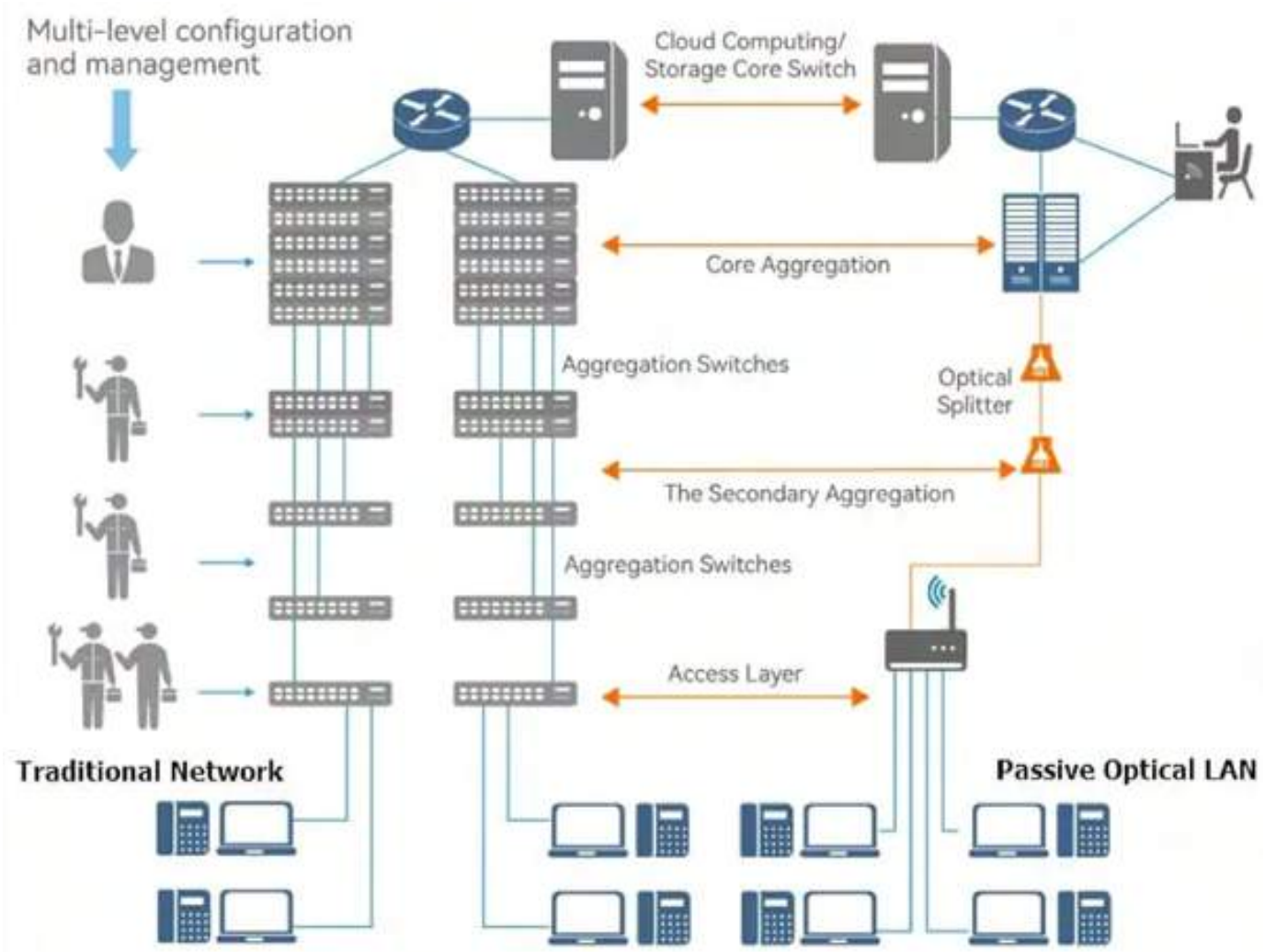
Najczęściej wykorzystywana w dostępie do źródeł danych jest infrastruktura Metro Ethernet, oparta na strukturze połączeń „punkt – punkt" oraz „punkt – wiele punktów" z prędkością do 10Gbit/s. W związku z opisanymi potrzebami rozwoju AI **nastąpią zasadnicze zmiany w infrastrukturze budowanej w Data Center, a także w sieciach budynkowych, przemysłowych i kampusowych.**

Kluczowym stanie się przygotowanie sieci konwergentnych, rozwiązań z możliwie małą ilością aktywnych urządzeń i przyjąć należy, że jedynym rozwiązaniem, które będzie w stanie sprostać tym wymaganiom będą Pasywne Sieci Optyczne – PON (POLAN).



POLAN to znana od dawna w sieciach dostępowych technologia, która dzięki dynamicznemu rozwojowi w ostatnich latach do standardu XGS-PON (ITU-TG.9807.1) umożliwia symetryczną transmisję danych z prędkością ~10 Gb/s. Kluczowymi zaletami technologii jest dystans między węzłem centralowym a terminalem abonenckim, który dochodzi do 60 km oraz żywotność >20 lat. W strukturze POLAN brak aktywnych węzłów pośrednich: mamy tylko jednostkę centralową OLT (Optical Line Termination), pasywne splittery optyczne i terminale abonenckie ONT (Optical Terminal Unit).

źródło: https://www.vsolcn.com/blog/passive-optical-lan.html



Architektura POLAN jest także technologią bezpieczniejszą niż konwencjonalne sieci LAN/WAN, z uwagi na wykorzystanie światłowodów, które gwarantują bezpieczeństwow warstwie fizycznej na poziomie zgodności z wymaganiami HIPAA oraz PCI DSS. Standard POLAN realizuje rozbudowane mechanizmy bezpieczeństwa: szyfrowanie danych przy pomocy AES, Access Control List, Broadcast Datagram Rate, autentykację urządzeń ONT oraz silne uwierzytelnianie w warstwie fizycznej danych i portów użytkownika, co ogranicza możliwość złośliwych działań.

POLAN wciąż ewoluuje: pilotażowe wdrożenia kolejnych generacji oferują już transmisję symetryczną 50Gbps (50GPON), a możliwość zastosowania WDM zwiększa wydajność pojedynczego włókna światłowodowego.

POLAN jest technologią znacznie tańszą z uwagi na małą liczbę urządzeń aktywnych. Centralne zarządzanie, od OLT do ONT jest zaletą nie do przecenienia. System PON oferuje żywotność wynoszącą 20 do 30 lat . Z tego powodu całkowity koszt posiadania (Total Cost of Ownership) wynosi zazwyczaj około 30% kosztów systemów Active Ethernet LAN. Zawdzięczamy to szczególnie znacznemu zmniejszeniu zajętości tras kablowych i brakowi węzłów pośrednich, które skutkuje znaczącym zmniejszeniem zużycia energii.

Po badaniu przeprowadzonym w Niemczech, Komisja Europejska nazywa światłowód „najbardziej energooszczędną technologią szerokopasmową" w porównaniu z innymi rodzajami kabli. Przy szybkości 50 Mb/s połączenia światłowodowe emitują 1,7 tony CO_2 rocznie, podczas gdy najlepsza opcja realizowana na kablach miedzianych emituje 2,7 tony. Zatem przejście na światłowód może natychmiast zmniejszyć emisję dwutlenku węgla o 1 tonę rocznie"[3].

[1] Worldwide IDC Global DataSphere Forecast, 2024–2028: AI Everywhere, But Upsurge in Data Will Take Time by Adam Wright https://www.idc.com/getdoc.jsp?containerId=US50554523
[2]https://www.forbes.com/sites/rscottraynovich/2024/01/23/what-ai-means-for-networking-infrastructure-in-2024/
[3]https://blog.frontier.com/2022/09/how-does-choosing-fiber-internet-benefit-the-environment/

8D. GRUPA T2S

Rosnąca rola outsourcingu w zarządzaniu infrastrukturą IT.

W raporcie "Mapa Trendów Data Center" zwraca się uwagę na rosnącą złożoność zarządzania infrastrukturą IT, co sprawia, że coraz więcej firm decyduje się na outsourcing tych zadań do wyspecjalizowanych podmiotów.

Chociaż na pierwszy plan wysuwa się zapotrzebowanie na wysoko wykwalifikowanych specjalistów IT, równie istotną rolą jest support pracowników niewyspecjalizowanych. Zdaje się taka teza dość górnolotnie postawiona, jednak prawdą jest, iż pracownicy fizyczni są częścią outsourcingu procesowego, w którym jednym z elementów jest zapewnienie codziennego wsparcia operacyjnego w obszarze bezpieczeństwa jej przestrzeni, m.in: poprzez prawidłową logistykę wewnętrzną, czystość, przepustowość ciągów komunikacyjnych, itd.

Grupa T2S, jako lider w outsourcingu procesowym i pracowniczym, dostrzega, że pracownicy fizyczni odgrywają jedna z ważniejszych ról w utrzymaniu bezpieczeństwa przestrzeni zarówno wewnątrz i na zewnątrz centrów danych. Choć to technologia i systemy informatyczne są sercem tych obiektów, ich sprawne funkcjonowanie nie byłoby możliwe bez odpowiedniego zaplecza zapewnionego przez personel fizyczny.

Pracownicy odpowiedzialni za utrzymanie czystości: Centra danych muszą spełniać rygorystyczne normy czystości, aby zminimalizować ryzyko uszkodzeń sprzętu spowodowanych przez kurz i inne zanieczyszczenia. Stąd cykliczne zapewnienie utrzymania czystości na wymaganym poziomie jest czynnikiem niezbędnym do utrzymania prawidłowego środowiska pracy dla urządzeń IT.

Pracownicy odpowiedzialni za logistykę: Kolejnym kluczowym aspektem jest logistyka wewnętrzna, która obejmuje transport i zarządzanie dostawami sprzętu, a także jego instalacją na miejscu. Pracownicy fizyczni odpowiedzialni za te zadania muszą w pierwszej kolejności przejść kilkuetapowe szkolenia stanowiskowe, tak aby móc pracować z tak specjalistycznym sprzętem – w fazie jego dostarczenia czy przenoszenia w określone miejsca.

Zarządzanie przestrzenią i konserwacja: Optymalne zarządzanie przestrzenią w centrum danych jest kluczowe dla zapewnienia

wydajności energetycznej oraz bezpieczeństwa operacyjnego. Pracownicy odpowiedzialni za zarządzanie przestrzenią i bieżącą konserwację infrastruktury fizycznej centrów danych pełnią istotną funkcję, dbając o to, aby infrastruktura była zawsze w odpowiednim stanie technicznym. Grupa T2S dostarczając takich pracowników, przyczynia się do minimalizacji ryzyka awarii oraz do zapewnienia ciągłości operacyjnej centrów danych.
Podsumowując, outsourcing zadań związanych z infrastrukturą IT w centrach danych obejmuje nie tylko zaawansowane usługi technologiczne, ale również kluczowe wsparcie operacyjne zapewniane przez firmy zewnętrzne. Tu najistotniejsza jest spójna korelacja na wielu płaszczyznach operacyjnych, która współtworzy całość procesów związanych z odpowiednim funkcjonowaniem centrów danych. Specjaliści IT, aby realizować powierzone im zadania muszą mieć zapewnione odpowiednie warunki pracy, które z kolei zapewniają im firmy outsourcingowe poprzez swój fizyczny personel.

9. AUTORZY

Autorka i redaktorka naukowa:
Kamila Pendyk

Współautorzy: Adam Wnorowski, Anna Tryfon-Bojarska, Katarzyna Blachowicz, Norbert Karmowski, Krzysztof Szczygieł, Jakub Kulesza, Konrad Hennig, Izabela Taborowska, Rafał Kittel, Kamil Klepacki oraz Marta Cudziło

Wywiady:
Anna Streżyńska, Jacek Siemiończyk oraz Piotr Kowalski

Case studies: Jakub Madej, Andrzej Tokarzewski oraz Olga Budziszewska

Komentarze: Renata Wozba i Marlena Svensson (Grupa T2S), Jacek Kłonica, Krzysztof Piotrowski, Michał Kandziora (S4Tech), Wiesław Wilk (Związek Polska Chmura)

Współpraca metodologiczna: dr Weronika Przecherska-Marchwińska, dr Anna Tryfon-Bojarska

Wsparcie merytoryczne i metodologiczne: Dagmara Krzesińska

Redakcja: Aleksandra Zacharska, Adam Wnorowski, Konrad Hennig

Korekta: Aleksandra Zacharska

Skład: Joanna Skaźnik-Honsek (QQ Design Studio)

8.10.2024 r.

ISBN 978-83-950595-2-0