CHMURA OBLICZENIOWA. KLUCZ DO BEZPIECZNEJ PRZYSZŁOŚCI?

Wiesław Sokół
UNICARD SA

Czy chmura jest bezpieczna? Mimo coraz nowszych rozwiązań technologicznych, wiele firm wciąż ma opory przed przeniesieniem danych poza własne, fizyczne środowisko IT. Postawmy więc na fakty. Przywołując case studies i statystyki rozwieję wątpliwości na temat bezpieczeństwa chmury obliczeniowej.

Czy chmura jest bezpieczna? Mimo coraz to nowszych rozwiązań technologicznych, wiele firm wciąż ma opory przed przeniesieniem danych poza własne, fizyczne środowisko IT.

Postawmy zatem na fakty. Przywołując case studies i statystyki postaram się rozwiać wątpliwości na temat bezpieczeństwa chmury obliczeniowej, na które wpływ mają ochrona dostępu do danych, fizyczne zabezpieczenia, jakość działania chmury czy ochrona pod kątem utraty danych.

POLSKA W NIECHLUBNYCH RANKINGACH

Analiza raportów i badań niestety nie pozostawia złudzeń – zdecydowana większość polskich firm z pewną dozą nieufności podchodzi do technologii chmurowych.

Według statystyk:

- tylko 7% firm w Polsce uważa swoją dojrzałość w chmurze za wysoką (PwC);
- jedynie 38% firm w Polsce wdrożyło chmurę we wszystkich lub większości swojej działalności (PwC);
- wydatki firm na usługi świadczone w modelu chmurowym stanowią aktualnie około 15% budżetów (Chmura obliczeniowa w Polskim e-biznesie, 2023).

Opór przed przeniesieniem poza własne, fizyczne środowisko IT wynika głównie z obaw o powierzenie wrażliwych danych zewnętrznej firmie oraz komplikacje związane z potencjalną zmianą dostawcy usług chmurowych – na takie powody zwróciło uwagę aż 32% badanych z wyżej wymienionego raportu.

Czy słusznie? Jak pokazują **badania**, w niemal 90% przypadków winę za naruszenia bezpieczeństwa chmury ponosi... błąd ludzki, a nie dostawcy chmury.

CORAZ BARDZIEJ WYRAFINOWANE ATAKI

Jak widać, polskie firmy mają spore obawy związane z możliwością przedostania się ich prywatnych danych w niepowołane ręce. Jednak niestety często nie idzie to w parze z należytą dbałością o cyberochronę.

Kilka tygodni temu głośno zrobiło się na temat ataku ransomware na ogólnopolską sieć ALAB Laboratoria. Hakerzy RA World udostępnili wrażliwe dane medyczne i personalne kilkudziesięciu tysięcy Polaków i Polek. To niestety jednak dopiero przedsmak ich planów – grupa zapowiada, że jeśli nie otrzyma okupu (którego wielkość wynosi rzekomo kilkaset tysięcy dolarów), na swoim blogu udostępni kolejne wrażliwe informacje.

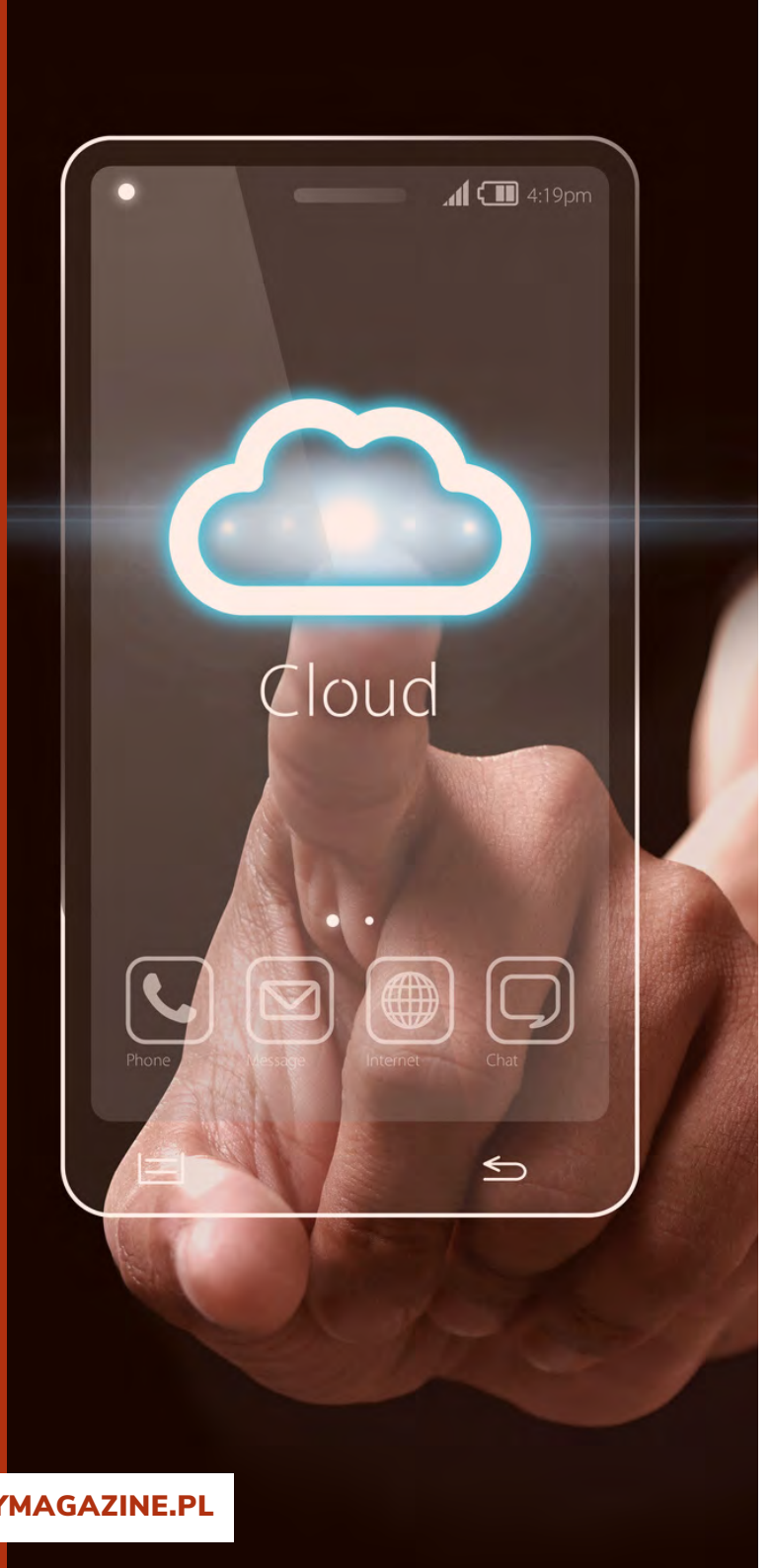
Z kolei pod koniec zeszłego roku światło dzienne ujrzała szokująca informacja – chińska grupa Chimera, niezauważona przez ponad dwa lata, infiltrowała sieć holenderskiego giganta półprzewodników. Naruszenie pozostało niewykryte do końca 2019 roku, tym samym narażając firmę na ogromne straty finansowe oraz wizerunkowe.
Jak widać, ataki cybernetyczne stają się nie tylko coraz bardziej śmiałe, ale niestety też skuteczne.

W ciągu ostatnich lat w Polsce hakerzy byli realnym zagrożeniem dla takich firm jak m.in.:

- Castorama;
- mBank;
- Allegro;
- Orange.

Incydenty dotknęły nawet instytucji rządowych jak Krakowa Rada Komornicza. W 2022 włamano się też na witrynę internetową polskiego Sądu Najwyższego.

Kto ponosi odpowiedzialność za te ataki? Trudno w takiej sytuacji nie oczekiwać od zhakowanych firm, aby z maksymalną uważnością dbały o bezpieczeństwo danych swoich klientów, pracowników, użytkowników czy pacjentów. Jednak, jak wynika z badań przeprowadzonych przez KPMG, w 2022 roku nawet **58% firm w Polsce doświadczyło ataku hakerskiego**. W tym samym roku do CERT Polska zgłoszono aż o 176% więcej ataków w porównaniu z rokiem 2021.



To pokazuje, że cyberataki stały się jednym z największych zagrożeń dla polskiego biznesu, który często nie jest gotowy na to, aby móc się przed nimi chronić.

PKO BANK POLSKI, POLSAT: GIGANCI PRZECIERAJĄ SZLAKI

Na szczęście dobre praktyki w kwestii bezpieczeństwa są coraz częściej wybierane i promowane przez topowe marki. Kilka miesięcy temu największy pod względem aktywów bank w Polsce – PKO Bank Polski – udowodnił swoje zaufanie do publicznej chmury obliczeniowej, przenosząc tam swoje zasoby IT.

Współpraca PKO BP z Chmurą Krajową zaowocowała migracją danych, zapewnieniem wsparcia oraz monitorowania przeniesionego systemu. Dzięki temu bank zaimplementował innowacyjne i efektywne technologie, osiągając wyższy poziom bezpieczeństwa oraz redukując koszty związane z utrzymaniem i modernizacją swojej infrastruktury.

Kluczowe jest, że terminale używane przez personel banku podczas interakcji z klientami służą jedynie jako punkty dostępowe, gdyż wszelkie obliczenia i transakcje odbywają się w chmurze. To upraszcza zarządzanie dużą liczbą sprzętu i obniża koszty zużycia energii elektrycznej. Jednak, co najważniejsze, taka konfiguracja znacząco wzmacnia bezpieczeństwo i ochronę przetwarzanych danych.

Na transformację cyfrową postawiła też Grupa Polsat. Co więcej, wykorzystywane przez nią rozwiązania są zasilane zieloną energią! W ramach współpracy z Polsat, Google podpisze swoją pierwszą w Polsce umowę na zakup czystej, ekologicznej energii elektrycznej.
- *Inwestycje w rozwój czystych, odnawialnych źródeł energii to praktyczna realizacja naszej strategii ESG* – mówi **Piotr Żak, wiceprzewodniczący Rady Nadzorczej Grupy Polsat Plus**.

Swoje usługi na chmurze opierają też takie marki jak Netflix, Airbnb, Spotify, Twitter, a nawet zaawansowane systemy bezpieczeństwa jak kontrola dostępu **impero 360**, przechowywana na Microsoft Azure, z którego korzysta aż 95% firm z listy Fortune 500, m.in. Audi czy Bosch.

Podjęcie decyzji o przejściu "do chmury" być może wielu polskich firmom ułatwi niedawne posunięcie Microsoftu, który kilka miesięcy temu otworzył pierwsze w Polsce (a nawet Europie Środkowo-Wschodniej) centrum przetwarzania danych w chmurze. To aż trzy niezależne lokalizacje w rejonie Warszawy, a każda z nich zawiera jedno lub więcej centrów danych. Co więcej, wszystkie lokalizacje zapewniają najwyższą jakość w kwestii prywatności, bezpieczeństwa oraz przechowywania danych zgodnie z obowiązującymi w Polsce przepisami.

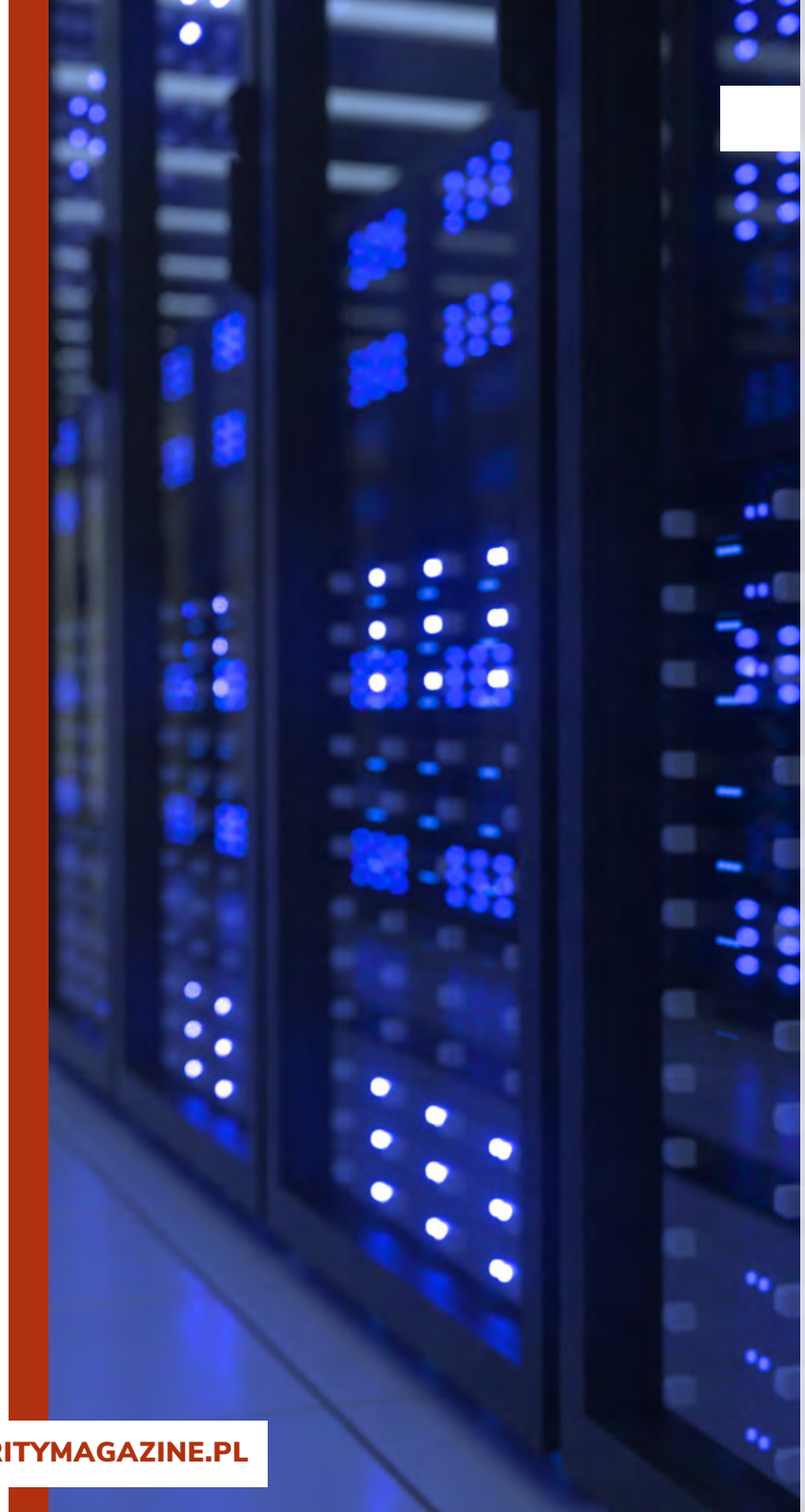
DYREKTYWA NIS2 ZMIENI WSZYSTKO?

Dyrektywa NIS2 (Network and Information Systems Directive 2) to aktualizacja unijnej regulacji z 2016 roku mającej na celu zwiększenie poziomu cyberbezpieczeństwa w Unii Europejskiej.

NIS2 rozszerza zakres obowiązków dla dostawców kluczowych usług i firm cyfrowych, w tym firm chmurowych, platform cyfrowych i dostawców usług internetowych. Zmierza do:

- ujednolicenia standardów bezpieczeństwa na poziomie europejskim,
- wprowadzenia rygorystycznych wymogów w zakresie zarządzania ryzykiem i zgłaszania incydentów,
- zwiększenia odpowiedzialności i przejrzystości działań firm w kontekście cyberbezpieczeństwa.

Dyrektywa nie wymusza bezpośrednio stosowania rozwiązań chmurowych.



Jej głównym celem jest zapewnienie wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych, wykorzystywanych przez podmioty kluczowe dla gospodarki i społeczeństwa. Oznacza to, że organizacje muszą stosować odpowiednie środki bezpieczeństwa, ale sposób ich wdrożenia zależy od indywidualnej oceny ryzyka i specyfiki danej organizacji.

Jednakże, w praktyce, wiele organizacji może uznać, że wykorzystanie rozwiązań chmurowych od renomowanych dostawców może pomóc w spełnieniu wymogów bezpieczeństwa określonych w dyrektywie NIS2. Chmury obliczeniowe często oferują zaawansowane narzędzia bezpieczeństwa, które mogą być trudne lub kosztowne do zaimplementowania we własnej infrastrukturze.

ZATEM... CZY CHMURA JEST BEZPIECZNA?

Wróćmy jednak do kluczowego pytania o bezpieczeństwo chmury obliczeniowej.
Po wielu latach pracy ze środowiskiem Microsoft Azure – w tym jako dostawca rozwiązania opartego o tę technologię – mogę śmiało wyrazić swoje zaufanie do chmury. Wynika ono nie tylko z zaawansowanych, wielowarstwowych zabezpieczeń, stałego backupu danych oraz redundacji środowiska, ale też faktu, że rozwiązanie jest ciągłe monitorowanie przez setki specjalistów Microsoftu.

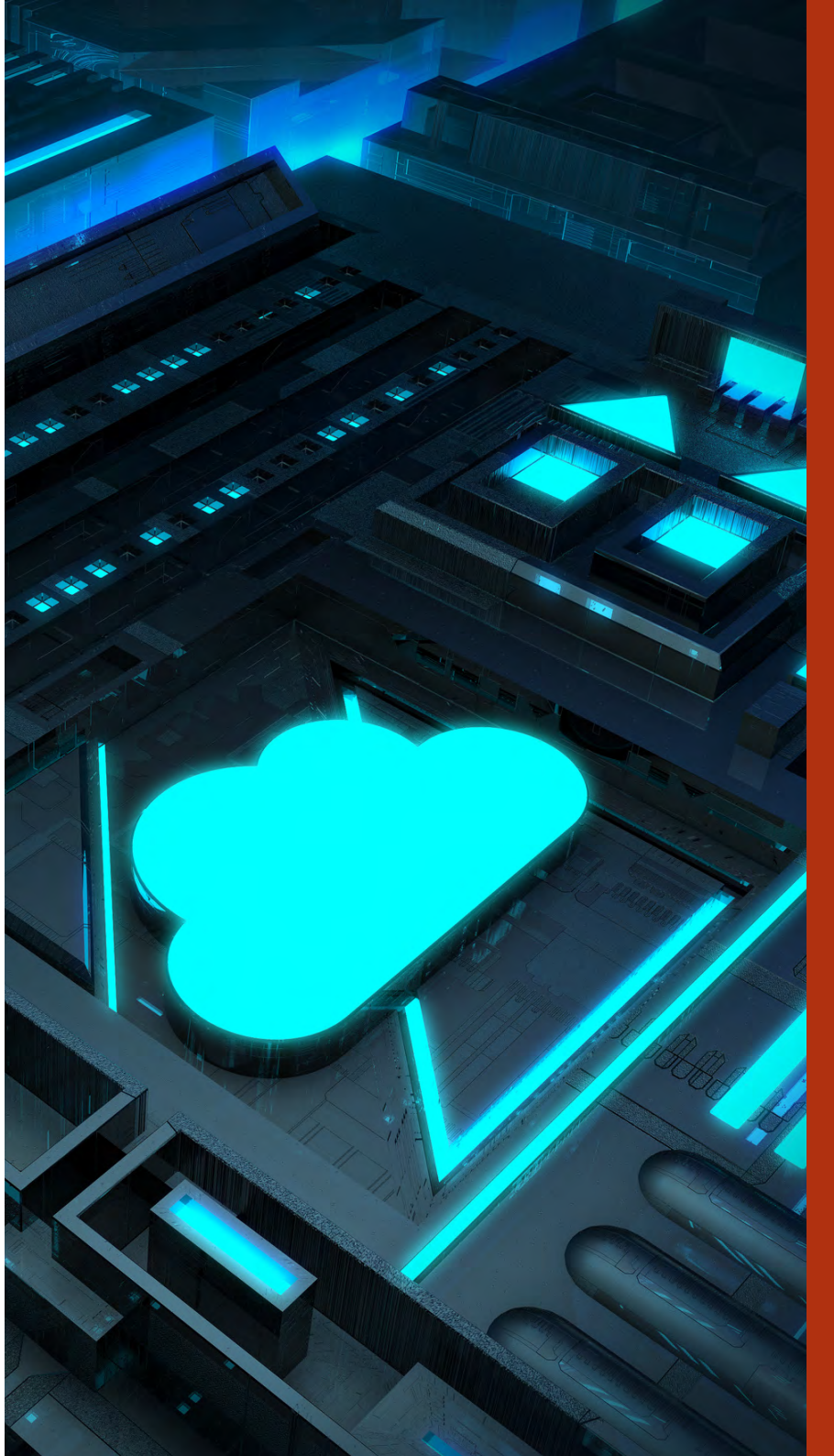
Nie można też pominąć dodatkowych zalet, jak:

- **ekologia** – chmura dynamicznie dzieli zasoby pomiędzy aplikacje, co powoduje maksymalne wykorzystanie zasobów. Dostawcy chmury dbają też o to, aby jak najwięcej zużywanej energii elektrycznej pochodziło ze źródeł odnawialnych. Pozwala to m.in. na obniżenie śladu węglowego.

Wybierając chmurę, dołączamy do grona firm, które kreują przyszłość kolejnego pokolenia oraz promują świadomość ekologiczną;

- **elastyczność** – klient nie ponosi nakładów na zakup infrastruktury i w każdej chwili może ograniczyć lub zrezygnować z części rozwiązania;
- **zawsze aktualna wersja oprogramowania** – użytkownicy chmury nie muszą dbać o aktualizację oprogramowania systemowego i aplikacji oraz nie ponoszą kosztów takiej usługi;
- **zgodność z przepisami prawa** – zmiany prawa mogą wymuszać zmiany w aplikacji. W przypadku chmury to producent zawsze odpowiada za tę kwestię;
- **bezpieczna kopia danych** – korzystając z chmury nie trzeba się martwić, że dane zostaną utracone lub backup się nie uda;
- **stały dostęp do zasobów i wydajność** – środowisko chmurowe jest w pełni wydajne bez względu na to, ile osób na nim pracuje.

Jak wynika z raportu Cybersecurity Insiders z 2023 roku o bezpieczeństwie chmury, inne czynniki, które skłaniają do rozważenia rozwiązań opartych na chmurze, obejmują zwiększoną skalowalność (54% respondentów), przyspieszony czas wdrożenia (52%) oraz oszczędność kosztów (41%).



Warto też pamiętać, że we wielu przypadkach na poziom bezpieczeństwa środowiska chmurowego ogromny wpływ ma sam użytkownik. Błędna konfiguracja czy niedostateczna ochrona danych uwierzytelniających mogą sprawić, że rozwiązanie będzie podatne na złośliwe działania lub incydenty czy naruszenia nie zostaną wykryte odpowiednio szybko.

Jednak najnowsze technologie w kwestii bezpieczeństwa, nowe oficjalne dyrektywy, a przede wszystkim – decyzje topowych firm, jak wspomniany PKO Bank Polski – pokazują, że rewolucja w stronę chmury jest nieunikniona. Im szybciej firmy zdecydują się na ten krok, tym lepiej dla środowiska i nich samych.