

As you wish – As a Service

[00:00:07]

Prowadzący: Cześć. Witam wszystkich słuchaczy naszego podcastu. Dzisiaj razem z moim gościem bierzemy na cel chmury, w wielu odmianach, ale na pewno nie będziemy bujali w obłokach, a raczej twardo stąpali po ziemi, przedstawiając Państwu, czym jest chmura, dla kogo opłacalne jest wykorzystanie chmury i co najważniejsze jak sprawić, by te złe i niedobre chmury były bezpieczne dla nas, użytkowników? As you wish – As a Service. Czy chmura to najlepszy przyjaciel działów IT? Dzisiejszym gościem jest mój imiennik – Michał Furmankiewicz, Head of Consulting Architekt Chmurowy w firmie Chmurowisko.

Michał Furmankiewicz: Dzień dobry.

Prowadzący: Cześć Michał. Dzięki za Twoją obecność. Myślę, że mogę o Tobie powiedzieć, że jesteś maniakem chmur, biorąc pod uwagę ilość lat, w których jesteś zaangażowany w pracę, jako Cloud Solutions Architect.

Michał Furmankiewicz: Tak, zdecydowanie. To jest coś, co lubię robić, co robię i ciągle praktycznie siedzę w środowiskach chmurowych. Także, mimo, że tytuł mógłby wskazywać na to, że już tylko zarządzam ludźmi, to ciągle aktywnie pracuję.

Prowadzący: Michał oprócz pracy w chmurowisku, czym jeszcze się zajmujesz, na co dzień? Jakie są Twoje zadania?

Michał Furmankiewicz: Oh. Ja tak naprawdę żyję, można powiedzieć, że trochę żyję tym co robię cały czas, bo oprócz tego, że pracuję jakby z chmurami, to staram się budować kominki wokół chmury w Polsce, także tym też się zajmuję. Udzielam się na konferencjach, także cały czas gdzieś tam te tematy wokół chmury.

Prowadzący: Czyli również szeroko pojęta edukacja?

Michał Furmankiewicz: Zgadza się, zgadza się. Edukacja, budowanie trochę rynku pewnie też.

Prowadzący: Świadomości.

Michał Furmankiewicz: Świadomości, zdecydowanie.

Prowadzący: Michał, zanim dotrzemy bezpośrednio do tematu - czy chmura to najlepszy przyjaciel działów IT, chciałbym zapytać o kilka elementów, od których myślę, że warto byłoby zacząć w ogóle nasze dzisiejsze spotkanie. Chmura, na razie w odniesieniu do chmury publicznej, tak?

Michał Furmankiewicz: Tak.

Prowadzący: Zawężmy sobie do chmury publicznej. Jako definicja, która no też nie będę ukrywał, jest mocno splotona.

Michał Furmankiewicz: Tak.

Prowadzący: To od razu zaznaczam. Jest czymś relatywnie prostym. Czyli udostępnianie zasobów bądź usług, w zamian za odpowiednie opłaty. Natomiast rzeczywistość jest znacznie bardziej skomplikowana.

Michał Furmankiewicz: Tak.

Prowadzący: Szczególnie porównując do czasami rzeczywiście niewybrednych memów, tak, które mówią, że nie ma chmury, tylko są czyjeś komputery. Najczęściej są to jakieś minusy.

Michał Furmankiewicz: Tak jest.

Prowadzący: Do kogo tak naprawdę są skierowane rozwiązania chmurowe?

Michał Furmankiewicz: Myślę, że dzisiaj ten rynek jest dużo szerszy niż kiedyś. Bo kiedy w 2008 roku AWS budował swój marketing wokół chmury mówił *AWS is for builders*, czyli mówił, że dla tych, którzy budują rozwiązania SASowe, budują aplikacje na chmurze. Potem Microsoft zaczął tę samą strategię przyjmować, mówiąc, że tak naprawdę, jeżeli chcesz robić in scale, jeżeli chcesz budować aplikacje na całym świecie, to chmura jest dla ciebie. Dzisiaj w zasadzie chmura zarówno jest wykorzystywana przez mniejsze firmy, które zaczynają budować swoje rozwiązania, przez średnie organizacje, które potrzebują gdzieś tam zwinności, ale też przez bardzo duże korporacje, które szukają jakby takiego wybiegu do przodu, nie kolejnej rearchitektury swojego środowiska IT, tylko innego pomysłu na dostarczanie usług do klientów końcowych i do wnętrza. Więc w zasadzie dzisiaj można powiedzieć, że od najmniejszych firm, po największych gigantów ludzie korzystają z chmur. Kropka. Tak naprawdę bardzo szerokie rozwiązanie.

Prowadzący: Czyli tak naprawdę w chwili obecnej nie ma jakiegoś progu wejścia, gdzie...

Michał Furmankiewicz: Powiedzmy, że Ty, jako indywidualny kupujący, jako indywidualna osoba, która potrzebuje być może jednej prostej strony, nie znajdziesz niczego dla siebie. Ale jeżeli na przykład już masz jakiś większy kawałek infrastruktury albo prowadzisz małą działalność gospodarczą i potrzebujesz usług SASowych, tak jak ja, na przykład ja. No to ja dzisiaj nie wyobrażam sobie budowania gdzieś tam serwera pocztowego czy innego [niepewne] serwera, tylko po prostu wykorzystuje to, co jest gotowe. Więc ja polegam w 100% na SASach. I takie firmy jak Chmurowisko widzę, że co raz bardziej po prostu chcą mieć pokupowane rozwiązania, a nie budować, budować wokół tego jakąś infrastrukturę.

Prowadzący: Słuchaj, chmura prywatna vs chmura publiczna.

Michał Furmankiewicz: Tak.

Prowadzący: Vs jeszcze hybryda, bo jeszcze oczywiście możemy mówić o hybrydzie.

Michał Furmankiewicz: Tak.

Prowadzący: Wady i zalety poszczególnych typów i w jakich sytuacjach najlepiej się sprawują, szczególnie, jeżeli chodzi o chmurę hybrydową, która no myślę czasami może powodować pewne niejasności, tak, jeżeli chodzi o samą koncepcję i budowę.

Michał Furmankiewicz: Tak. Myślę, że nie mamy tyle czasu. A tak zupełnie szczerze...

Prowadzący: Przypuszczam, że moglibyśmy tutaj rozmawiać przez godzinę.

Michał Furmankiewicz: Tak, tak, tak. Spokojnie. Znaczący myślę, że dłużej. Ja bym powiedział w ten sposób, ja dzisiaj na pewno nie będę wiarygodny, jeżeli chodzi o ocenę chmury prywatnej. A to z tego względu, że gdzieś moja wizja tego jak to działa zatrzymała się w 2014 roku. Natomiast to, co, gdzie widzę jakby jeszcze dzisiaj, niemożliwość działania w chmurach publicznych, jeżeli Ty masz workloady bardzo stare, legacy, które z różnych powodów nie są migrowane do środowisk publicznej chmury, jeżeli masz system oparty o inny architektoniczny x86, jeżeli potrzebujesz bardzo specyficznej konfiguracji swojego sprzętu bądź wydajności, to być może jeszcze dzisiaj lepszym rozwiązaniem będzie coś, co masz on – premises, co w 100% kontrolujesz. Chociaż już w chmurach publicznych pojawiają się permetal, pojawiają się rozwiązania VMRowe, SAPowe, również may framowe [niepewne], co jest pewną ciekawostką.

[00:05:00]

Michał Furmankiewicz: Natomiast tam, gdzie potrzebujesz 100% kontroli, cokolwiek to jest, to prawdopodobnie rozwiązanie on - premises będzie tym lepszym rozwiązaniem. Gdzie cloud publiczny będzie trudny do pobicia? Zawsze tam, gdzie jest Ci potrzebna instant scale, czyli duża skala, bardzo szybko powoływana, gdzie Ty chcesz oddać komuś, dać pieniądze komuś za to, że buduje usługi passowe, czy gotowe usługi do wykorzystania swoich rozwiązań, których Ty nie musisz budować, to tam ciężko będzie wygrać z chmurą publiczną, moim zdaniem. I tam gdzie chcesz zmienić trochę model dostarczania usług, czyli chcesz dostarczać jeszcze szybciej i nie wymyślać koła na nowo, to tam na pewno cloud publiczny będzie łatwiejszy w adopcji. Hybryda jako taka? Trudno powiedzieć jeszcze teraz gdzie będzie ona bardziej wartościowa, gdzie mniej, bo trzeba zdefiniować, czym jest hybryda. I tu przepraszam, ale...

Prowadzący: Dokładnie. Od tego zacznijmy.

Michał Furmankiewicz: Tak.

Prowadzący: Czym jest ta hybryda, jeżeli chodzi o chmurę?

Michał Furmankiewicz: Kiedyś mój partner w biznesie powiedział coś takiego, że hybryda to jest wszystko, co nie jest ani w 100% on - premises, ani w 100% w chmurze. Więc można gdzieś powiedzieć, że hybryda to jest każda sytuacja, w której nie wiemy-wykorzystujemy jedną tożsamość w wielu miejscach; wykorzystujemy wielu dostawców chmurowych, bo to też jest hybryda swojego rodzaju; budujemy rozwiązanie, które być może jest zintegrowane sieciowo, na poziomie sieciowym jest rozwiązaniem on – premises. Więc trudno powiedzieć, gdzie ta hybryda się kończy, a zaczyna, bo to jest każda kombinacja architektury on – premises chmurowej plus dostawców innych chmurowych tak naprawdę. I teraz ta hybryda w wielu miejscach jest ciekawa. Bardzo dzisiaj wielu klientów bankowych mówi – Michał, chmura-tak. Ale wolelibyśmy żeby do Internetu i ruch z Internetu przechodził przez nasz bank, bo my mamy wszystkie rozwiązania, kupowane od różnych Vendorów, dostawców,

którzy potrafią fajnie filtrować nasz ruch. Chmura hybrydowa tak, bo na przykład chcemy używać Azure Cloud [niepewne] w jednym rozwiązaniu, co się daje robić. Więc to są te miejsca gdzie potrzebujesz zalet kilku rozwiązań, gdzie hybryda powiedzmy, jest interesującym miejscem rozwiązania.

Prowadzący: Słuchaj, dlaczego tak naprawdę chcemy migrować w tym momencie nasze środowiska i usługi do chmury? I czy jest to spowodowane jakimś trendem, który co raz częściej oczywiście widać – chmura tu, chmura tam?

Michał Furmankiewicz: Mhm, tak.

Prowadzący: Czy jest to spowodowane wygodą dostępu do zasobów? Czy jest to spowodowane kwestiami właśnie związanymi z bezpieczeństwem, o tym jeszcze za chwileczkę pewnie porozmawiamy, ale na zasadzie redundacji plus przeniesienia pewnej odpowiedzialności na providera, rachunki, czy coś jeszcze tutaj?

Michał Furmankiewicz: Właśnie tu jest ciekawa sytuacja. Nawet pokusiłem się w nowym roku o zrobienie takiej prezentacji, która pokazywała jak się cloud zmieniał od wielu lat. I to co było interesujące, czyli migracja, o której zacząłeś mówić do środowisk chmurowych, była ciekawa na rynkach zachodnich w 2013 - 2014 roku, kiedy Capital One [niepewne] migrowało się w 100% do AVSa, u nich agregacja [niepewne] do 2 były fajnym business casem. W Polsce raczej nikt nie patrzy, bo jeżeli mówimy o rynku polskim na przykład, to ludzie nie patrzą na to – migrujemy się do chmury. Raczej – spróbujmy zrobić rearchitekturę rozwiązań, zbudować rozwiązania, które natywnie potrafią wykorzystać zalety środowisk chmurowych i przenieśmy je tam. Dlaczego? Z wielu powodów – ucieczka do przodu, jak powiedziałem; rearchitektura rozwiązań ze względu na inne oczekiwania; bardzo często pojawiająca się koncepcja mikroserwisów, która ma w założeniach, bo nie zawsze to się daje robić, dostarczać szybciej; plus wykorzystanie gotowych usług, czyli niewymyślanie koła od nowa. To jest bardzo często powtarzany case właśnie w środowiskach, w Polsce na przykład.

Prowadzący: Wiesz co, teraz chciałbym jeszcze wrócić do mojego wcześniejszego pytania i do kwestii związanych z architekturą on-prem. Czy rozwiązania on-prem według Ciebie mają swoje najlepsze lata już za sobą? I jeżeli już to, co tak naprawdę chcemy zachowywać na swoich serwerach? Czyli podobny przykład, o którym wspominałeś, który z jednej strony chce inwestować w chmurę, ale z drugiej strony mówi, że ale pewne rzeczy zostawiamy jednak u siebie.

Michał Furmankiewicz: Ja myślę, że pomysł na to, że takie bardzo duże instytucje i takie tradycyjne, kiedyś w 100% będą w chmurze, to dzisiaj są trudne do wyobrażenia sobie, z różnych względów. Natomiast, więc na pewno ten on-premises zostanie, będziemy go bardziej automatyzować. Na pewno automatyzacja to jest taki klucz w ogóle w chmurze i on-premises, więc jeżeli on-premises zostanie będzie bardziej automatyzowany, będzie dalej, bardziej powoływany przez cloud, ale na pewno zostanie też na dość długo z nami, choćby ze względu na te uwagi, które wcześniej wspominałem. To nie zniknie jutro.

Prowadzący: Wspominałeś o zmianach w architekturze.

Michał Furmankiewicz: Tak.

Prowadzący: Związanych z migracją.

Michał Furmankiewicz: Tak.

Prowadzący: Tutaj właśnie, na jakie pułapki najczęściej podczas migracji możemy się nadziać?

Michał Furmankiewicz: Na całe mnóstwo. Bo tutaj możemy sobie pozwolić myśleć, że na taką też otwartość zupełnie. Czasami ten marketing Vendorów pokazuje, że to wszystko jest przecież proste, łatwe i w sumie to jutro zmigrujemy całą firmę. Szczęśliwie dzisiaj ci Vendorzy, też powiem inaczej – nie jest tak, że dziś, jutro zmigrujemy całą firmę. Po pierwsze, cloud ma w ogóle inną koncepcję, tam dostępność nie jest gwarantowana przez urządzenia, tylko przez nadmiarowość infrastruktury. Pewne koncepcje skalowania chociażby, nie robimy scale out, tylko, znaczy nie scalujemy jednej instancji, tylko dokładamy kolejne instancje. To jest inne podejście w ogóle do projektowania systemów.

[00:10:08]

Michał Furmankiewicz: Mamy całą gamę usług gotowych, więc pytanie na przykład czy odtwarzać nasze rozwiązanie backupowe, które mamy on-premises w chmurze. Więc tu jest wiele takich decyzji, które trzeba sobie zadać w kontekście architektury. Inna opcja to jest jak dobrać w ogóle usługi w środowisku chmurowym versus to co mamy on-premises. To nie są rzeczy, które są 1:1 mapowane. No niby wirtualna maszyna, wirtualna maszyna, dość powiedzieć, że na przykład tylko w Microsoft Azure jest 462 wielkości maszyn wirtualnych. Pytanie, jak to zmapować? Więc problem jest wielowymiarowy, jeżeli można tak powiedzieć, o, tak naprawdę.

Prowadzący: Chciałem jeszcze zapytać o rosnące wpływy. I tutaj platform as a service (PaaS), infrastructure as a service (IaaS), software as a service (SaaS).

Michał Furmankiewicz: Tak.

Prowadzący: Wady i zalety w porównaniu do rozwiązań on-prem, to jest pierwsza sprawa. I czym tak naprawdę między sobą różnią się te rozwiązania w kontekście od możliwości jakie dają klientom te poszczególne modele usługowe? Do jakich zadań najlepiej sprawdza się dany model?

Michał Furmankiewicz: Szerokie pytanie. To zacznijmy po kolei, spróbuję to poukładać. Platform as a service (PaaS) versus software as a service (SaaS). PaaS to platforma, czyli gotowe już usługi wyższego rzędu niż czysta infrastruktura, na bazie których budujesz aplikacje. Na przykład baza danych, jako usługa, system do monitorowania typu APM – Applications Performance Management, jako usługa; wstęp do wgrywania podatności jak usługa, etc. Czyli gotowe komponenty, które nie dają żadnej wartości biznesowej końcowemu użytkownikowi, ale z których taka osoba jak ja potrafi łatwiej poskładać rozwiązania. Jak popatrzymy na rozwiązania typu na przykład Bankowo, Goodie na polskim rynku, czy, czy to, co robi Vodeno na przykład. Oni właśnie korzystają z passów tam, gdzie chcą przyspieszyć czas dostarczania rozwiązań. SaaS – gotowe usługi biznesowe, z których użytkownik

końcowy, taki jak Ty, czy ja, czy moja żona potrafi je wziąć i zacząć korzystać, tak. Czyli tam gdzie chcemy mieć instant wdrożenie, prawie instant wdrożenie i korzystać z gotowej funkcjonalności biznesowej – proszę bardzo, office 365. Trochę saftware [niepewne]. Chociaż tutaj mam wiele wątpliwości, mówiąc te słowa, bo to jest jednak zawsze dopasowanie do klienta, ale nie wiem, prostsze rozwiązanie. Więc jest cała masa SaaSowych, gotowych komponentów, produktów, które biznes może kupić i teoretycznie sam zacząć korzystać. No i teraz, jeżeli pytasz o wady, zalety, no znowu, to jest tak naprawdę pytanie - co my chcemy osiągnąć? Ja zawsze zadaję sobie takie pytanie, ja i klientom je zadaję-jaki jest cel, jaki problem chcemy rozwiązać, jaki jest ten rzeczywisty problem? Bo czasami moim zdaniem definiujemy problemy, które nie są tymi właściwymi problemami do rozwiązania. Jeżeli my chcemy na przykład dzisiaj nie zajmować się więcej utrzymaniem poczty, utrzymaniem Internetu, być może, utrzymaniem jakichś rozwiązań okołobiznesowych, to być może Office 365 świetnie rozwiązuje ten problem. I widać u klientów w Polsce, że to rzeczywiście tak działa. Jeżeli my chcemy dać naszym deweloperom komponenty, z których mogą wybudować szybciej swoje rozwiązania, czyli platformę, to dodajemy im na przykład zarządzany klaster Kubernetesa, którego nie trzeba stawiać, nie trzeba utrzymywać, tylko jest jakby ready to use po pierwszych 5 minutach od wdrożenia. Więc tu trzeba by było zadać sobie pytanie właśnie jaki problem rozwiązujemy i wtedy dobrać rozwiązanie do problemu pewnie, tak.

Prowadzący: Słuchaj, mam teraz mocno podchwytliwe i myślę kontrowersyjne pytanie. Czy ludzie dalej bardzo boją się chmury? Szczególnie, jeżeli chodzi tutaj o kwestie bezpieczeństwa, które są mi szczególnie bliskie. Czy klienci dojrzewają do chmury, czy to chmura się zmienia i dzięki temu staje się bardziej atrakcyjna? I wiesz, do czego też od razu, od razu mówię, do czego piję, tak?

Michał Furmankiewicz: Mhm, tak.

Prowadzący: Ponieważ ja często się spotykam z takim przeświadczeniem. Myślę, że Ty również.

Michał Furmankiewicz: Tak.

Prowadzący: Że jako bezpieczeństwo to tylko on-prem. No szczególnie, jeżeli chodzi o takie typowo sieciowe kwestie związane z bezpieczeństwem, to jest tylko i wyłącznie on-prem. I ludzie chyba często zapominają, tak z mojej perspektywy, że własne data center może być mimo wszystko gorzej chronione niż zasoby przytrzymywane właśnie w chmurze. To jest pierwsza sprawa. Czy to pod kątem bezpieczeństwa fizycznego, czy to również właśnie bezpieczeństwa przed atakami cyberprzestępców tak naprawdę. Druga sprawa, w jaki sposób obecni producenci rozwiązań bezpieczeństwa właśnie sami wykorzystują chmurę, o czym też często zapominamy, wydaje mi się.

Michał Furmankiewicz: Tak jest, tak jest.

Prowadzący: Albo chcemy zapomnieć, bo to jest drugi scenariusz. A chmura towarzyszy nam nawet wtedy, kiedy sobie z tego tak naprawdę nie zdajemy sprawy.

Michał Furmankiewicz: No i znowu kilka, kilka jakby pytań w jednym, więc spróbujmy zacząć od początku, czyli od tej kwestii czy ludzie się boją chmury. Ja to znowu jestem trochę złą osobą do zadania takiego pytania, z prostego względu. No ja budzę się rano i zaczynam korzystać z chmury, kończę wieczorem i pracuję z klientami, którzy korzystają z tych chmur, więc pewnie nie widzę tej drugiej strony. Ale trzeba powiedzieć jedną rzecz, zajmuję się chmurą 7 lat. 7 lat temu, to było jak dowcip, który gdzieś tam krąży. Dzisiaj jest raczej pytanie, nie czy korzystać, tylko jak korzystać mądrze, w kontekście danej organizacji, jak to robić bezpiecznie. To ja bym powiedział, że zupełnie się zmieniło nastawienie i też to co pewnie Ty też słyszałeś Michale, chmura nas zwolni – ludzi albo zredukuje ludzi. [00:15:04]

Prowadzący: Oczywiście.

Michał Furmankiewicz: Chmura nie zwolni ludzi, chmura ich zatrudni więcej, za inne stawki i chmura powiększy poziom komplikacji naszych środowisk. Dlatego, że wprowadzamy hybrydowość, czyli wielość usługową. No i teraz w kontekście bezpieczeństwa. Ja myślę, że dzisiaj ludzie, którzy są świadomi tego jak dzisiaj działa, działa cyberprzestępczość, tak naprawdę wykorzystują chmurę właściwie bardziej właśnie po to, żeby być w stanie przeanalizować wszystkie te zdarzenia, które się dzieją i żeby wykrywać potencjalne próby ataków, czy też zdarzenia, które mogą prowadzić do incydentów, niż odwrotnie. Znaczą cloud jest idealnym miejscem do tego, żeby te rzeczy, zdarzenia przetwarzać. Czy cloud może być mniej bezpieczny niż moje data center? Można pytanie postawić. Oczywiście, że może. Z prostego powodu, zawsze ten powód bardzo często jest pomiędzy klawiaturą, a krzesłem. To znaczy 88% błędów związanych z bezpieczeństwem chmury to jest po stronie użytkowników, a nie po stronie dostawców. Oczywiście, że dostawcy nie są nieomylni. Nie ma takich dostawców. Nieomylna to jest tylko moja żona, wiadomo. Więc zdarzają się błędy po ich stronie, ale większość przecieków, wycieków danych, czy też jakby błędów jest spowodowanych tym, że my nie umiemy tego konfigurować, tak naprawdę.

Prowadzący: No to przykład właśnie z tych takich bardziej flagowych Capital One Finance.

Michał Furmankiewicz: Tak.

Prowadzący: No wyciek olbrzymi, no chyba jeden z takich rzeczywiście, najbardziej flagowych.

Michał Furmankiewicz: Mhm.

Prowadzący: Podobna sytuacja. Tak jak opisujesz. No błąd tak naprawdę nie jest ze względu na błędy service providera, czy na architekturę albo...

Michał Furmankiewicz: Użytkownika.

Prowadzący: Kwestia użytkownika. Jest błąd konfiguracji.

Michał Furmankiewicz: Tak. Ja myślę, że chmura na pewno ma w jednym miejscu, jest czasami bardziej ryzykowna, ponieważ wiedzę o środowiskach on-premises budowaliśmy kilkadziesiąt lat, już dzisiaj tak naprawdę kilkadziesiąt lat. O chmurze budujemy ją lat 7, czy tam 8, czy 10 niektórzy i co więcej, ta

chmura się zmienia. To myślę, że to jest teraz takim, taką trudnością, że ta chmura się zmienia, a my nie nadążamy z budowaniem kompetencji, żeby to robić właśnie w sposób poprawny i bezpieczny, po prostu.

Prowadzący: Wiesz co, zostańmy dalej w kwestiach związanych z bezpieczeństwem. I teraz chciałbym Cię zapytać o takie elementy, które też są newralgiczne, czyli związane z segmentacją zasobów, z dostępem do danych. Jak to jest organizowane?

Michał Furmankiewicz: To zależy mocno od providera. Natomiast jakby to, co jest istotne i to u każdego providera występuje, każdy provider mówi coś takiego – chcesz korzystać z chmury, zrób sobie coś, co providerzy nazywają Foundation, czyli taką bazową architekturę środowiska chmurowego, gdzie właśnie zdecydujesz – jak posegmentujesz sieć; na jaki ruch pomiędzy segmentami sieci pozwolisz; czy ten ruch będziesz zbierał i odkładał gdzieś [niepewne]; być może jakieś urządzenie typu tap [niepewne] sobie wprowadzisz; jak posegmentujesz uprawnienia, komu te uprawnienia dasz; czy będziesz mógł je elewować, czyli podwyższać sobie czasowo, czy nie; jak będziesz zabezpieczał tożsamość. 92% znowu, ataków na tożsamość wynika z braku drugiego składnika. No dzisiaj to jest standard. To jest cała koncepcja passwordless, czyli biometryczne jakieś urządzenia, które pozwalają Ci tą tożsamość przenosić. I o tym wszystkim się właśnie dyskutuje, zanim się zacznie korzystać ze środowisk chmurowych, czyli model uprawnień, model tożsamości, model sieci, monitoring tego środowiska, rejestracja incydentów, praca nad incydentami. To wszystko można przygotować. Również kwestia podziału danych, o której wspominałeś. Więc to trzeba po prostu wypracować. I są w każdym cloudzie jakieś mechanizmy, które pozwalają też to kontrolować i nakładać pewien standard. Czy na przykład polityki organizacyjne, które pozwalają Ci wymusić, że konfiguracja rozwiązań jest taka albo żadna. Czy też na przykład role, które pozwalają Ci powiedzieć – z tych usług możesz korzystać, z tych nigdy nie będziesz mógł korzystać, tak. Więc można te rzeczy sobie bardzo precyzyjnie poukładać u każdego dostawcy, tak żeby ten cloud był już taki bardziej nasz niż providera. Nie taki z pudełka, tylko dopasowany do naszej organizacji. To można zrobić.

Prowadzący: Mówiłeś o tych największych graczech. A co tak naprawdę z mniejszymi operatorami, którzy świadczą podobne usługi?

Michał Furmankiewicz: Znaczą właśnie. I tutaj myślę, że trzeba sobie wyjaśnić jedną rzecz, tak bardzo precyzyjnie. Jeżeli weźmiemy tych największych, tą pierwszą trójkę z Gartnera, czyli Amazon Web Services, Microsoft Azure i Google Cloud Platform, chociaż tam jeszcze Alibaba się gdzieś kryje. To trzeba sobie powiedzieć, że AWS to jest prawie 200+ usług, Microsoft Azure to jest ponad 170, Google jest na poziomie gdzieś 70 usług. Więc pytanie, że jak zestawiamy to z mniejszymi dostawcami, to czy porównujemy jabłka do jabłek. To jest podobna koncepcja wynajmowania usług i zasobów na czas za pieniądze, ale już detale są bardzo, bardzo różne. No i oczywiście skala inwestycyjna jest zupełnie, zupełnie inna, tak. Więc ci mniejsi dostawcy są, będą, mają swoje miejsce. Oni są bardziej dedykowani

do konkretnych jakichś zastosowań. Natomiast mają też bardzo ciekawe usługi i na pewno rynek będzie bardzo heterogeniczny w tym zakresie. Dominacja jest jasna, nie da się jej już nadgonić, a jedna z firm, bardzo dużych próbowała dwa razy i po dwóch razach prezes firmy stwierdził, że tempo jest tak duże, że nawet gdyby wydać ogromną ilość pieniędzy, nie da się nadgonić tego już, tego co się dzieje.

[00:20:08]

Prowadzący: Wspomniałeś jeszcze, praktycznie na samym początku naszej rozmowy o jednej, dla mnie przynajmniej, bardzo interesującej rzeczy, czyli o backupie. Tutaj pytanie – czy chmura nadaje się do backupu? I też od razu wyjaśniam, do czego chcę zmierzać. Wykorzystanie chmury do backupów versus backupy na miejscu, czasami bez odpowiedniego zabezpieczenia, bez odpowiedniej segmentacji. I wiesz no, głupi scenariusz, tak. Wpada Ransomware i nagle okazuje się, że nie ma danych i ups, backupu też nie ma, abstrahując od jakichś rozwiązań typu Raid ones, prawda bądź kolejnych przypadków i żartów, choć mających jakieś tam odzwierciedlenie w realiach, tak. Czyli zaszyfrowaliśmy Ci dysk, tak – tak, wiem, mam backup. My też wiemy i też mamy swój backup. Więc w tym momencie wiesz, następuje z reguły cisza. Właśnie chmura, jako przechowywanie backupu.

Michał Furmankiewicz: Są tego typu rozwiązania. Natomiast no to znowu, trzeba znowu wejść w detale. Jest jedna z dużych firm w Polsce z branży e-commerce, która przechowuje backup laptopów w cloudzie. Z prostej przyczyny, no nominalnie nigdy tego nie robili, bo po co backupować laptopy użytkowników, nie ma na to nigdy pieniędzy i teraz to zaczęli robić. Czy można robić coś bardziej poważnego? Budowałem architekturę, która zakładała przeniesienie 400 Tera danych backupowych do środowiska chmurowego. Bo dzisiaj już dostawcy backupów potrafią działać w ten sposób, że istniały jeszcze rozwiązania [niepewne] on-premises, a on potrafi te dane odkładać do środowiska chmurowego, przy okazji szyfrować, deduplikować dane.

Prowadzący: No właśnie, to jest kwestia duplikacji czy po prostu natywnego wsparcia?

Michał Furmankiewicz: Nie, natywnego, natywnego wsparcia. Oczywiście, wiadomo, backup to jest bardziej złożony proces. Te backupy, których rzeczywiście potrzebujemy ongoingowo, są raczej odkładane lokalnie. Potem te zimniejsze, być może na jakichś mniejszych środowiskach lokalnie. Ale te po miesiącu raczej nie są wykorzystywane bieżąco, nie są odkładane do środowiska chmurowego. Więc jak najbardziej takie akcje, które są budowane. Kwestia oczywiście przeliczenia kosztów i sprawdzenia, czy polityka, którą stosujemy backupów i odtwarzania, na które trzeba mieć licencję. Taki głupi dowcip. Po prostu wpisuje się w to podejście i tyle, tak.

Prowadzący: A słuchaj, kto tak właściwie jest odpowiedzialny za zabezpieczenie chmury? Gdzie tak naprawdę kończą się możliwości i oczywiście obowiązki dostawcy, a zaczyna się własne pole do manewrów, do zagospodarowania, do wrzucenia wszelakich zabezpieczeń, administracji? No tak bezpośrednio przez klienta.

Michał Furmankiewicz: No i tutaj to znowu zależy troszeczkę od providera, bo ci providerzy są różni. Ale jakby wszyscy ci najwięksi providerzy, którzy budują te cloudy publiczne, mówią, że to jest [niepewne] model. I pokazują takie diagramy, w których w zależności od typu usługi, który wybierasz, do pewnego poziomu to jest dostawca. Czyli fizyczne bezpieczeństwo, prawda. Sama fizyka serwerów, te klatki wszystkie, które są zbudowane, redundancja łączy internetowych, odprowadzania ciepła, czy w ogóle energii. Plus te wszystkie jakby rzeczy, które się kojarzą z fizyką, to na pewno zapewnia dostawca. Potem oczywiście zapewnia bezpieczeństwo na warstwie wirtualizacji. Tam są z reguły dwie warstwy wirtualizacji, o tym dostawcy nie mówią zbyt chętnie, ale.

Prowadzący: Bo nikt nie lubi się dzielić tym co ma.

Michał Furmankiewicz: Tak. Tam się nie dzielą. Natomiast można takie rzeczy złapać pomiędzy słowami. Polecam tutaj zarówno sesje tych dostawców na wszystkich tych konferencjach. Oni o tym jednak mówią. Notabene, też jest inny ciekawy wątek, ale to może później. W każdym bądź razie, do poziomu systemu operacyjnego z reguły to robi dostawca. Od poziomu systemu operacyjnego w górę, robisz to Ty. I to jest właśnie ten [niepewne] model. Jeżeli Ty nie umiesz zabezpieczyć maszyny, nie patchujesz jej, a otwierasz port, są znane podatności, ale oczywiście tego nie zrobisz, no to trudno mieć zarzut do Vendra, że po prostu popsujesz swoje wdrożenie. Natomiast w usługach passowych, większość znowu tego ciężaru utrzymania systemu operacyjnego przechodzi na dostawcę chmurowego. I tam sprawa zaczyna się komplikować, bo w zależności od usługi, ten poziom swobody może być różny. Więc tutaj nie mam jednej, dobrej odpowiedzi, bo...

Prowadzący: Wszystko zależy od modelu.

Michał Furmankiewicz: Ciągłe zależy bardzo od modelu, bardzo zależy. Oczywiście w tych usługach SaaSowych praktycznie 100% tego aspektu bierze na siebie dostawca z drobnymi uwagami. No, jeżeli ktoś nie zabezpieczy tożsamości, pozwala korzystać na niezabezpieczonych być może komputerach, no to jakby tutaj już dostawca nie pomoże.

Prowadzący: No to sprawa raczej jasna.

Michał Furmankiewicz: Tak, tak, tak.

Prowadzący: Słuchaj, jakie narzędzia dostarczają globalni operatorzy dla zabezpieczenia swoich chmurowych instancji? Co można wykorzystać? Chmura, jako taka powiedzmy biała kartka do zagospodarowania, jeżeli chodzi o kwestie no zabezpieczeń firm trzecich również, tak. Czyli oferty producentów, cały marketplace, firewalle, IPS, WAFY, ochrona aplikacji i tak dalej.

Michał Furmankiewicz: No właśnie i tu jest ciekawie, bo jakby dostawcy mówią tak, że po pierwsze oni dostarczają ilość gotowych rozwiązań. I to też jest fajne dla mnie, bo widać, że z roku na rok tych rozwiązań natywnych jest co raz więcej, w zakresie ochrony tożsamości, wykrywania zdarzeń na maszynach, wykrywania prób przełamania właśnie warstwy 7 czy 4 w zakresie sieciowym.

[00:25:03]

Michał Furmankiewicz: Więc dostawcy dostarczają cały szereg rozwiązań swoich bezpieczeństwa. Natomiast, i tutaj może jeszcze jeden ciekawy komentarz. Dostawcy mają bardzo szerokie spojrzenie na to, co w ogóle w tym bezpieczeństwie się dzieje. Microsoft mówi, że dziennie analizuje 18 miliardów zdarzeń bezpieczeństwa, które spływają ze wszystkich jego rozwiązań chmurowych, jakby outputy tego, co wykryje jako podatność trafiają do produktów, których używa. Ale drugi aspekt tego, żeby się nie zabezpieczać tylko dostawcą. Tutaj jak powiedziałeś – marketplace. Właściwie jest już wszystko, bo właściwie każdy większy dostawca bezpieczeństwa oferuje coś swojego w modelu appliance. Czy to właśnie WAFY, czy urządzenia typu IDS, IPS, czy rozwiązania, które wspierają procesy tapowania sieci, czy rozwiązania typu DLP, czy rozwiązania do utwardzania sieci, do hardeningu sieci, do wykrywania podatności. W zasadzie każdy dostawca już coś ma. I to jest też fajne, bo budując rozwiązania dla dużych, naprawdę enterprisywnych klientów, można powiedzieć – wybierzcie to, co lubicie, zobaczymy jak to się integruje z danym inventorem chmurowym i wykorzystajmy wasze już kompetencje, wasze know-how, do tego żeby sobie zabezpieczać waszą infrastrukturę chmurową. Jest taka linia cienka, gdzie dostawcy klasyczni jeszcze nie wchodzą. To są właśnie wszystkie rozwiązania passowe. Dlatego, że tam, mimo wszystko model dostarczania rozwiązań jest inny i tamci dostawcy nie mają bardzo często dostępu do tych warstw, które chcieliby monitorować. Więc tu jest jakaś taka linia, gdzie trzeba zawierzyć to Vendorowi i jego natywnym rozwiązaniom. Ale mówię, wykorzystanie marketplace jest przeogromne dzisiaj.

Prowadzący: Czyli z jednej strony rozwiązania natywne od service providera, a z drugiej strony tak naprawdę to, co klient lubi, co klient zna i to, co klient chce uzyskać.

Michał Furmankiewicz: Tak. I to, co pasuje do architektury. No jeszcze wiesz, jedna ciekawa rzecz się dzieje. To może nie jest takie widoczne, ale Vendorzy chmurowi zaczynają też grać w inną grę. Na przykład Vendorzy chmurowi mówią tak – mam bardzo fajne rozwiązania bezpieczeństwa, zabezpieczę Ci jeszcze tą drugą chmurę i tą trzecią chmurę. Czyli można w jednym miejscu podłączyć sobie jeszcze GSP, i AWS, i jeszcze coś i monitorować to w jednym miejscu. Myślę, że ciekawe zagranie. I w drugą stronę daje się te logi natywnie przesyłać do tych rozwiązań chmurowych i analizować w jednym miejscu. Czyli jak budujesz Siema, nagle nie masz trzech siemów, w trzech chmurach, tylko masz jednego siema w jednej chmurze, mimo, że używasz trzech różnych providerów. To jest też myślę, że ciekawa rzecz, która się dzieje.

Prowadzący: Podejście dobre.

Michał Furmankiewicz: Tak. Inne będzie trochę bardziej kłopotliwe w utrzymaniu. Po prostu.

Prowadzący: Wszystko dla klienta. Słuchaj, jak bardzo podejście do bezpieczeństwa w chmurze musi się różnić od tego podejścia w stosunku do tego podejścia on-prem? W teorii sytuacja powinna wyglądać bardzo podobnie. Ale no środowiska jednak się mimo wszystko znacznie różnią między sobą.

Michał Furmankiewicz: Znacząca myśl, że tak jakby... Jak nie jestem bezpiecznikiem, by hard. Ja nie mam takiego doświadczenia. Zajmuję się tym tematem, bo jakby go lubię i interesuję się, ale nie jestem bezpiecznikiem by hard. Natomiast to, co mogę powiedzieć na pewno. Pewne podejścia są takie same, natomiast wiedza, którą trzeba mieć, żeby się tym zajmować jest inna. Dlaczego? Załóżmy taką prostą rzecz. Jak skoordynować [niepewne] jakieś usługi passowe? No to trzeba te usługi znać, wiedzieć, jakie mają modele odkształceń, no i zbudować sobie taki hardenik i na przykład tylko w takim modelu to wdrażać. Więc tutaj nie jest tak, że bezpiecznik, który zajmował się klasycznie bezpieczeństwem, na przykład sieci, od razu wie, co może zrobić w środowisku chmurowym. Bo pewne rzeczy są [niepewne], a pewne nie. Więc przede wszystkim usługi, zakres ich wykorzystania, architektura tych usług, to jest dosyć istotne. Druga, trzecia kwestia, druga kwestia, przepraszam, to jest to, co możesz użyć do monitoringu tych usług. Więc tutaj rzeczywiście, znowu jest tak, że niektóre rozwiązania będą za krótkie do pewnych usług passowych w środowiskach chmurowych. No i kwestia całego podejścia typu SM [niepewne], czyli incident management response. Tutaj też są gotowe natywne usługi. Nie zawsze ten nasz SM, który mamy on-premises, do którego prześlemy dane przez jakiegoś Event Huba, będzie tym najlepszym miejscem, żeby robić analitykę pod tego typu rozwiązania. Chociaż tutaj też trzeba powiedzieć, że rynek się zmienia, jak najbardziej. Bardzo znane SMy już dzisiaj integrują się z dostawcami chmurowymi, żeby to analizować. Więc, a trzeba mieć wiedzę, inne troszeczkę podejście, ale pewnie warsztat jest dosyć podobny, tylko zmieniają się usługi.

Prowadzący: A zgodność chmury z przepisami, regulacjami? Czyli tutaj tak naprawdę no cała lista. Począwszy od RODO, HIPAA, PCI DSS i tymi wszystkimi rzeczami. Jak operatorzy podchodzą do tych przepisów?

Michał Furmankiewicz: To jest ciekawe, bo operatorzy wzięli sobie to bardzo, bardzo do serca. I jak wejdziemy na stronę, wpisujemy w Google danego dostawcę i compliance to z reguły trafimy na stronę, która bardzo wyczerpująco pokazuje certyfikacje, które są dostępne u danego providera, zakresy usług, które mają tę certyfikację, bo tutaj gwiazdka, nie zawsze wszystkie usługi mają te same certyfikacje, bo się nie da tego zrobić. I zobaczymy też, że nawet po podpisaniu [niepewne] daje się uzyskać dostęp do raportów, które pokazują raport przeprowadzony z takiej analizy u Vendors.

[00:30:01]

Michał Furmankiewicz: Sprawa RODO jest kontrowersyjna, bo jak wiemy RODO to nie jest kwestia certyfikacji. To jest kwestia też architektury i tego jak przechowujemy dane w aplikacji. Więc RODO jest trochę takim tematem, że co z tego, że...

Prowadzący: Ciężkim [niepewne]

Michał Furmankiewicz: Tak, tak, tak. Natomiast, jeżeli chodzi o regulacje lokalne to też jest ciekawie. Vendorzy chmurowi dzisiaj mówią – my chcemy być zgodni z różnymi regulacjami lokalnymi. Na przykład pokazują jak odpowiadają na wymogi KNFu w Polsce. Azure, AWS, GSP, każdy z nich ma swoją

odpowieź. Więc Vendorzy też starają się dostosować do wymogów rynku lokalnego i wymogów branż lokalnych, żeby na to odpowiedzieć.

Prowadzący: Wiesz co, jeszcze wracam do wcześniejszego pytania, które też mnie mocno zainteresowało jeżeli chodzi o monitorowanie platform. Jak dostawcy dbają o monitorowanie swoich platform, a z drugiej strony o instancje klientów? I tutaj pytam w odniesieniu zarówno o monitoring tego ruchu do instancji klienta, ale również tego ruchu wychodzącego z instancji klienta, który może nosić w sobie jakieś znamiona niebezpiecznego. Na przykład, no nie wiem, różne mogą być elementy, hostowanie serwerów, czy infrastruktury do ataków, no scenariusze mogą być najróżniejsze. Jak sobie operatorzy też działają powiedzmy z tym monitorowaniem w drugą stronę?

Michał Furmankiewicz: W drugą stronę... No oczywiście znowu, dużo, dużo rzeczy nie wiemy. Nie jest to, nie jest to zdradzane. Natomiast na pewno wiemy tyle, że ruch zaczynam trafi do naszej instancji przechodzi przez 7 różnych warstw, które są dość dobrze opisane, w zakresie tego, że są najczęściej warstwy [niepewne] oczywiście na początku. Potem jakieś rozwiązania, które mają patrzeć na reputację adresów, z których ten ruch przychodzi. Potem oczywiście wykrywanie klasycznej takiej wolumetrii, TCP floody i tego typu historie. Dopiero potem adres naszej instancji IP, wycinanie całego ruchu, którego nie lubimy, czyli wszelkiego rodzaju tunelowania, [niepewne], te wszystkie rzeczy są wycinane. No i dopiero szczęśliwie nasz ewentualnie publiczny adres IP, jeszcze do tego gateway i dopiero nasza prywatna adresacja. Więc tu jest cały szereg urządzeń, o których niestety nie mam pojęcia, które nie są ujawniane w tym zakresie. No i w drugą stronę jest bardzo podobnie. Na pewno to, co widać po dostawcach, dostawcy monitorują wszelkiego rodzaju próby połączeń do instancji, które nie są nasze. I jeżeli na przykład, kiedyś z jednym z kolegów testowaliśmy sobie Malwary na Windowsach 10, w chmurze. Malwary się bardzo szybko rozprzestrzeniły. No i po dwóch dniach dostaliśmy [niepewne] ładnego, czerwonego maila, że chyba coś dziwnego robimy, bo zaczynamy skakać po klientach innych instancji – proszę to wyłączyć, albo skasujemy wam konto. Także Vendorzy na pewno ten ruch też monitorują i ten ruch starają się chronić klientów.

Prowadzący: Ale z pełną kulturą – proszę sobie sprawdzić, bo wydaje nam się, że coś niedobrego się dzieje.

Michał Furmankiewicz: Tak, tak, tak. No bo oczywiście, jest to, jeżeli ruch jest pomiędzy dwoma instancjami to nie zawsze musi być ten ruch, to nie musi być ruch negatywny, tak. No, ale jeżeli obserwujemy go dużo i nagle. I tu właśnie jest ciekawy case. Widać, że dostawcy chmurowi muszą działać na bazie wolumetrii, tam się nie da posadzić tony bezpieczników, którzy będą to przeglądać tylko albo mamy do tego narzędzia analizy dużych zbiorów danych i wykrywania anomalii wykorzystania uczenia maszynowego, no albo nie potrafimy monitorować bezpieczeństwa jakiegoś środowiska. Kropka.

Prowadzący: Dodatkowe możliwości, jakie daje chmura dla rozwiązań stricte bezpieczeństwa, jak producenci wykorzystują chmurę? Mówię tu o producentach rozwiązań właśnie bezpieczeństwa i to nie pod kątem powiedzmy marketplace, bo to już gdzieś było poruszone. Tylko jak oni po prostu wykorzystują te popularne, tych popularnych providerów chmurowych, do tego żeby świadczyć, no swoje usługi?

Michał Furmankiewicz: Mhm. Tutaj też jest ciekawie, bo okazuje się, że po prostu chmura jest dobrym miejscem z kilku powodów. Po pierwsze, jest dobrym miejscem do rozkładania ataków typu ditos, tak. No to, to jakby klasyka, od wielu lat to się robi i to nie jest żadna tajemnica. Chmura jest dobrym miejscem też do analizy właśnie tak jak powiedziałem, zdarzeń, które mamy i zbieramy z różnych miejsc. Jest dobrym miejscem zarządzania różnego rodzaju urządzeniami zbierania telemetrii z tych urządzeń, szczególnie jak budujemy rozwiązania globalne. Także dostawcy wykorzystują na wiele sposobów cloud. Też wykorzystują cloud żeby rozwijać swoje produkty, bo prawda jest dzisiaj taka, że nie jesteśmy w stanie w środowiskach on-premises przetestować pewnych scenariuszy, które wydarzą się w środowiskach chmurowych. Więc dostawcy też w ten sposób wykorzystują cloud, do tego. I ciekawe, co się wydarzy dalej. Tutaj mówię o tym, że ciekawe, co się wydarzy, bo wydaje mi się, że dostawcy też będą wykorzystywali chmurę w tym zakresie, żeby swoje produkty czynić bardziej bezpiecznymi, właśnie za pomocą swoich rozwiązań. Jak? Trudno mi jeszcze powiedzieć, ale to się dzieje, to się dzieje.

Prowadzący: Możliwości są.

Michał Furmankiewicz: Możliwości są, na pewno. Znaczący myślę, że też to, co widać po dostawcach bezpieczeństwa, że oni chcą też swoje produkty rozwijać w ten sposób, że nawet, jeżeli używamy produktu on-premises, to dobrze by było na przykład, w jednej konsoli móc utwardzać sieć on-premises i chmurową.

[00:35:03]

Michał Furmankiewicz: W jednej konsoli kontrolować WAFY on-premises i w chmurze. I to się dzieje już naturalnie.

Prowadzący: Pełna orkiestracja.

Michał Furmankiewicz: Tak, pełna orkiestracja. W jednym miejscu na przykład wykrywać podatności na instancjach on-premises, w Azure i w AWSie. I to się też dzieje, więc tutaj ten rynek jest gigantyczny.

Prowadzący: Michał, jeszcze pytanie, które mi też chodziło po głowie. Najciekawsze przypadki wykorzystania możliwości chmury, w polskich instytucjach. Takie, z którymi Ty miałeś po prostu do czynienia, nad którymi nie wiem, pracowałeś bądź o których słyszałeś. I gdzie tak naprawdę, no chmura zrobiła po prostu swoje, gdzie tak jak mówiłeś on-prem no, nie zdałby tutaj zadania, albo byłoby to wykonalne w znacznie dłuższym czasie?

Michał Furmankiewicz: Tutaj tego jest dosyć dużo w polskich instytucjach, paradoksalnie, chociażby cały system JPK. No wiele osób wie, że to jest hybrydowe rozwiązanie, gdzie właśnie inicjalny ruch, który generujemy jako firmy, składające deklaracje, przechodzi przecież przez cloud. Dopiero potem jest składowany w data center, które są zlokalizowane w Radomiu, bo tam Ministerstwo Finansów ma swoje data center. Dlaczego tak? No właśnie kwestia odparcia ataków, wyskalowania się na parę dni, dosłownie, w miesiącu. No i też kwestia szybkości dostarczania nowych wersji JPK. Przemek Koch, wiceprezes firmy Aplikacje Krytyczne, która jest aplikacją, firmą rządową, ostatnio pokazywał, że cały system nowy viaTOLL będzie bazował na rozwiązaniach chmurowych i oni to rzeczywiście robią. Także dla nich to jest po prostu możliwość budowania szybko i w dużej skali rozwiązań. Ale też dalej, chociażby ostatnie deklaracje PKO BP. PKO BP swoje dwa rozwiązania, których używają do obsługi klientów będzie budowało w środowiskach chmury publicznej i nawet być może nie dlatego, że to co mają on-premises, się nie sprawdza. Tylko oni po prostu chcą przez to sprawdzić, czy te wszystkie obietnice za chmurą są, dają się realizować. No i oni chcą w ten sposób zmieniać bank, ten bank ma być jeszcze bardziej cyfrowy, jeszcze szybszy i chmura ma być dla nich właśnie tym katalizatorem zmiany. Czy na przykład Vodedo, to jest bank postawiony na chmurze GSP, dostarczany do klientów w Belgii, postawiony totalnie przez Polaków, którzy pracują na południu Polski. Bank postawiony dosłownie w kilka miesięcy. To jest naprawdę szybko, jeżeli ktoś pracuje w tej branży, od 6 do 9 miesięcy powstał cały, kompletny bank, oferowany z GSP, z licencją właśnie w tamtym regionie świata. Ale też wiesz, tych produktów jest dużo. Nie wiem, chociażby to, co robi Pracuj.pl. Pracuj.pl to jest portal też postawiony na cloudzie i Maciej Chwiłoc mówi, że – dla mnie cloud to jest szansa analizy dużych zbiorów danych, w bardzo szybkim czasie i dzięki providerom, ja mogę to uzyskać. Po prostu, ja mogę rozwijać swój biznes. Także jest tego, jest tego dużo.

Prowadzący: Szansa dla big data.

Michał Furmankiewicz: Zdecydowanie. Duże zbiory danych czują się bardzo dobrze w środowiskach chmurowych. I niestety, nie mogę powiedzieć, która firma, ale mogę wam powiedzieć taką rzecz, że są firmy w Europie, które kiedyś były w stanie pewne agregaty liczyć raz na tydzień, raz na miesiąc i w ten sposób antycypować przyszłość. Dzisiaj, ta sama firma mówi – ja mogę z dokładnością każdego miejsca w Europie, których mamy wiele, z dokładnością dzienną, rozliczać zużycie zasobów i przyszłe zużycie zasobów, w tym jednym miejscu. I dzisiaj to już jest szybkość, tak. Ale mówią – za rok będziemy mieć co godzinę, bo my dostawę będziemy w ten sposób planowali. Brzmi abstrakcyjnie, ale dla nich, nawet zainwestowanie dużych pieniędzy w tego typu rzecz daje taką, daje po prostu gigantyczne oszczędności w łańcuchu dostaw. Niestety, nie mogę powiedzieć więcej o projekcie. Dzieje się już 1,5 roku. No, ale właśnie tego typu problemy zaczynałyby się rozwiązywać w środowiskach chmury publicznej.

Prowadzący: Jak wygląda separacja warstwy usług od warstwy fizycznej u tych głównym providerów chmurowych?

Michał Furmankiewicz: Ludzie, którzy odpowiadają za architekturę data center, nie pracują na miejscu w data center, nie pracują też w supportcie. Czyli te trzy role są zawsze rozłączne. Osoby, które pracują w data center nie mają dostępu do konsoli wsparcia klientów, nie znają też architektury logicznej tych rozwiązań. Także tu jest silna, silna separacja. No i dalej, na samym poziomie już dostarczania usług. No nie wiem czy wiecie, ale na przykład tożsamość wykorzystywana w środowiskach chmurowych trzymaną jest na oddedykowanych, innych zewnętrznie serwerach, fizycznych, które nie są, nie działają w tych samych miejscach, w których działa usługa chmurowa. Znowu same maszyny wirtualne przy ich tworzeniu, występują algorytmy rozrzucania tych maszyn po środowisku chmurowym, tak żeby nie dało się wyliczyć, na który fizyczny serwer ona wpadnie. Notabene, przy restarcie proces się również powtarza. To jest też ciekawe. Jeżeli składujecie dane w chmurze publicznej, no to te dane trafiają z reguły na kilka dysków. Na każdym z nich dane wasze są szyfrowane tym samym kluczem, ale dane innych klientów szyfrowane są innymi kluczami. Więc nawet jakby ktoś fizycznie ukradł ten dysk, to zobaczy wiele różnych danych, zaszyfrowanych różnymi kluczami. Więc też ciężko myśleć o procesie dekrypcji, bo to nie są też całe, całe grupy danych.

[00:40:10]

Michał Furmankiewicz: No i takich rzeczy jest sporo. Każdy dostawca robi to po swojemu. Nie zdradza oczywiście, co robi. Dzisiaj na przykład mamy dostawców, którzy mówią, że robią double encryption, czyli szyfrują dyski fizycznych maszyn, które utrzymują instancje chmurowe. I instancje chmurowe mają też szyfrowane dyski na poziomie właśnie tej warstwy składowania danych. Także wiele różnych aspektów tutaj.

Prowadzący: Wiesz co, to było bardzo ciekawe, co powiedziałaś. Ale teraz pojawiło mi się tak naprawdę bardzo proste pytanie, wiesz. Bo tak apropo właśnie dysków lokalizacji serwerów. Jeżeli przyszedłby do Ciebie klient i zapytał się – gdzie są przechowywane moje dane? Już nie mówiąc tutaj odnośnie konkretnego serwera, tylko powiedzmy jakiejś lokalizacji, to providerzy są w stanie mu odpowiedzieć na to pytanie?

Michał Furmankiewicz: Providerzy podają... Znaczą tak, Ty, jako klient wstawiasz swoje instancje w danej lokalizacji, więc Ty wiesz, gdzie wstawiasz, że wstawiasz w tym data center albo w innym data center. Provider też oczywiście, po stronie suportowej będzie znał informacje, na którymś tam poziomie, gdzie ta instancja jest przechowywana. Natomiast, tak naprawdę te informacje nie są wykorzystywane do suportów, w ogóle. Znaczą na przykład Ty, to co proponuję każdemu klientowi, żeby klient założył case supportowy i zapytał na jakim racku leży jego maszyna. To jest zawsze fajne, co support odpowiada.

Prowadzący: I co z reguły odpowiada?

Michał Furmankiewicz: Że nie może takiej informacji zdradzić, bo takiej informacji tak naprawdę nie ma. Po prostu, sam support, tak. Nie jest to wyliczalne przez ich perspektywę. Więc jesteśmy w stanie

wskazać data center, jesteśmy w stanie wskazać czasem availability zone, czyli logiczną lokalizację, ale nie jest zdradzona nigdy fizyczna lokalizacja tych danych. To jest też może ciekawe. Dużo tego, pewnie można by było jeszcze spokojnie jeden podcast nagrać.

Prowadzący: Michał, z Twojej perspektywy. Jeżeli chodzi powiedzmy o nowych klientów, takie typowe ABC, jeżeli chodzi o taką bezpieczną higienę pracy, tak, z chmurą. Aby rzeczywiście, w jakiś tam sposób czuć się lepiej, aby nie dopuszczać do wycieków danych. Więc tak znowuż, jeżeli moglibyśmy całość podsumować, w takich kilku słowach. Do czego tak najlepiej, rzeczywiście z powrotem, odbić się? Czyli odnośnie segmentacji, odnośnie wykorzystania danych, odnośnie tego, jakie dane wrzucamy i czy dokładnie wiemy, co tak naprawdę robimy ze swoją instancją.

Michał Furmankiewicz: I tutaj, trochę taką metodą zdartej płyty. Mam nadzieję, że już nie słyszeliście tego zbyt wiele razy. Znaczący, tutaj jest klasyka gatunku. Zaczynamy najczęściej od tożsamości, bo to jest klasycznie pierwszy perimenter w środowisku chmurowym. Potem, bardzo często pojawia się kwestia, o której wspominałeś – klasyfikacji danych, czy ryzyka, związanych z przetwarzaniem danych, danych w środowiskach chmury publicznej. I to w przypadku instytucji regulowanych trzeba spełnić. No a potem jest już jakby prosto. Dobór usług, z których my chcemy korzystać, bo nie potrzeba nam 160, więc może wyłączmy te, których nie potrzebujemy. Weźmy tylko te, które chcemy. Dobierzmy ich architekturę, w której będą się czuły dobrze. Być może, nie wiem, osadzimy wszystkie sieci, a może, a może jednak nie. Zastanówmy się nad tą architekturą sieciową. Pomyślmy o tym, jak będziemy je monitorować, jak będziemy monitorować te zdarzenia bezpieczeństwa. No i zrobimy pierwszego pilota, ja celowo mówię nie PoC, bo dla mnie PoC to są stracone pieniądze i czas. Tylko zrobimy pierwsze rozwiązanie, które rzeczywiście żyje, nauczymy się, zbierzmy wszystkie lessons learned i wszystkie błędy, powtórzmy cykl. No i już, no. To tyle.

Prowadzący: Bardzo Ci dziękuję za dzisiejszą rozmowę.

Michał Furmankiewicz: Ja bardzo dziękuję.

Prowadzący: Moim i Państwa gościem był Michał Furmankiewicz, z firmy Chmurowisko. Michał, wielkie dzięki.

Michał Furmankiewicz: Dziękuję.

Prowadzący: Drodzy Państwo, do usłyszenia w kolejnym odcinku. Hasłem dzisiejszej audycji była przyjazna chmura.