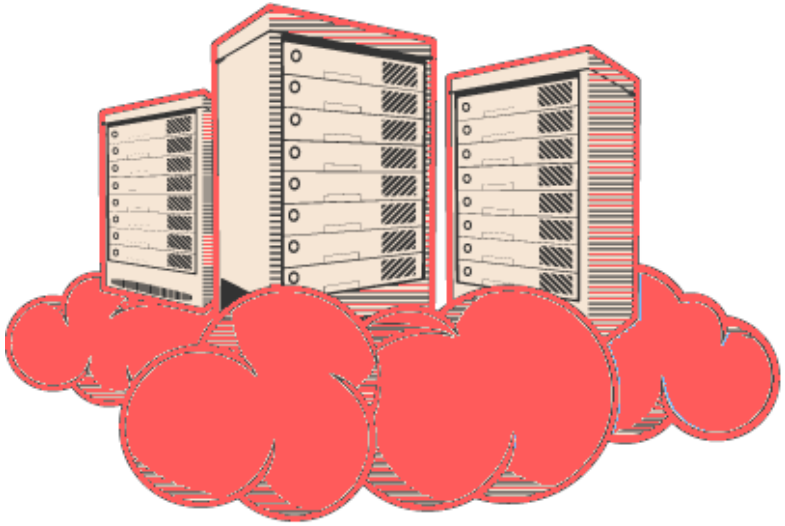
ISACA
Trust in, and value from, information systems
Katowice Chapter

„CLOUD COMPUTING, WYZWANIA I RYZYKA”



Adam Mizerski adam@mizerski.net.pl 507-071-401

ISACA
Trust in, and value from, information systems
Katowice Chapter

ADAM MIZERSKI:

Audytor, biegły sądowy, członek Izby Rzeczoznawców PTI a także ekspert z obszaru informatyki w zakresie wyceny środków trwałych oraz wartości niematerialnych i prawnych wartości spółek giełdowych realizowanych według wartości godziwej na potrzeby przygotowania sprawozdań finansowych według wymogów MSR / MSSF.

Pasjonat bezpieczeństwa (co współpracownicy nazywają obsesją) oraz metod (PN-ISO/IEC 27005:2010/Risk IT/COSO) oceny zintegrowanej analizy ryzyka, Główny Administrator Bezpieczeństwa Systemów oraz „karbowy XXI wieku" czyli szef działu IT.

AGENDA

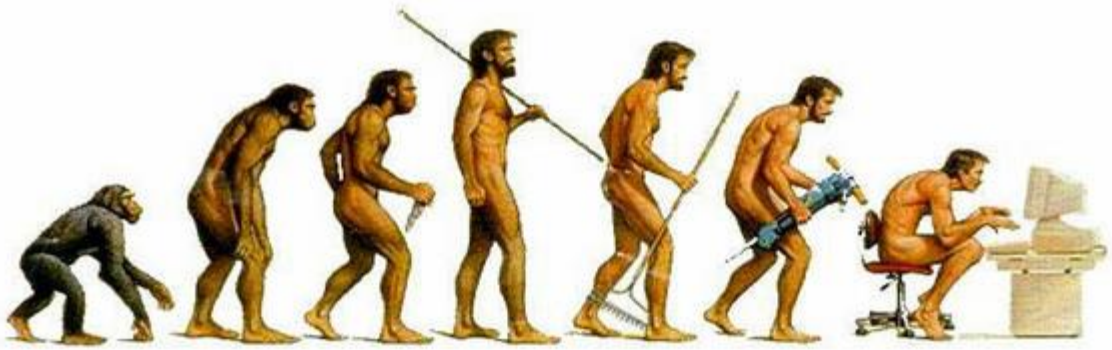
A. CLOUD COMPUTING

B. WYZWANIA

C. RYZYKA

D. KONKLUZJA

E. DYSKUSJA



SaaS

PaaS

IaaS

LEASING

KOLOKACJA

WIRTUALIZACJA

EWOLUCJA TECHNICZNA = EWOLUCJA RYZYKA

ISACA
Trust in, and value from, information systems
Katowice Chapter

Tradycyjne IT	Infrastructure (as a Service)	Platform (as a Service)	Software (as a Service)
Aplikacja	Aplikacja	Aplikacja	Aplikacja
Dane	Dane	Dane	Dane
Biblioteki wykon.	Biblioteki wykon.	Biblioteki wykon.	Biblioteki wykon.
Szyna danych	Szyna danych	Szyna danych	Szyna danych
Systemy operac.	Systemy operac.	Systemy operac.	Systemy operac.
Wirtualizacja	Wirtualizacja	Wirtualizacja	Wirtualizacja
Serwery	Serwery	Serwery	Serwery
Pamięci masowe	Pamięci masowe	Pamięci masowe	Pamięci masowe
Sieci	Sieci	Sieci	Sieci

EWOLUCJA TECHNICZNA = EWOLUCJA RYZYKA

ISACA
Trust in, and value from, information systems
Katowice Chapter

Dlaczego Cloud Computing to ulubione dziecko zarządów :

Koszty, koszty, koszty, ……

Przesunięcie wydatków IT z budżetu inwestycyjnego (CAPEX) do budżetu operacyjnego (OPEX)

Elastyczność

Krótki czas Time-to-market

Zgodnie z prognozami na rok 2013 przychody firm z branży IT związane z świadczeniem usług w chmurze to ok

8,3 mld zł

Raport „Cloud computing: Elastyczność, Efektywność, Bezpieczeństwo

http://www.microsoft.com/poland/administracja/Raporty.aspx

Public cloud

Private cloud

Hybrid cloud

Na początku było słowo/pytanie

Jaki jest akceptowalny

czas przestoju

systemów informatycznych naszej firmy

ODPOWIEDŹ NA PIŚMIE !!!

Na początku było słowo/pytanie

Jak cenne są

dla naszej firmy

dane

O ODPOWIEDŹ NA PIŚMIE BĘDZIE TRUDNO !!!

Czy wykorzystanie Cloud Compiuting

zagwarantuje nam zapewnienie ciągłości usług

oraz bezpieczeństwo danych ?

NIESTETY NIE ZAWSZE ☹

Case Study awarii e24cloud.com

https://www.e24cloud.com/static/casestudy

Disclaimer

Awaria środowiska produkcyjnego największej polskiej chmury obliczeniowej e24cloud.com dotknęła bezpośrednio tylko klientów, którzy nie zdecydowali się backupować swoich środowisk. Wspomniana grupa klientów nie skorzystała z żadnego z dostępnych sposobów, które umożliwiał panel zarządzania serwerami w chmurze e24cloud.com; tj. z usługi ustawienia automatycznego backupu wg harmonogramu lub backupu na żądanie, kosztującego 2,16 zł miesięcznie za 1GB danych.

Case Study awarii e24cloud.com

Czarny poniedziałek 4.06.2012

W poniedziałek, 4 czerwca 2012, w wyniku utraty ciągłości zasilania na obu torach zasilających DataCenter, w którym kolokowane jest e24cloud.com, nastąpiła krótkotrwała przerwa w zasilaniu macierzy dyskowych.

Z Sieci zniknęły m.in. Wykop.pl, Kwejk.pl, Money.pl, Oferia.pl, NaTemat.pl, Tablica.pl, Citeam.pl czy PayU.pl.

Case Study awarii e24cloud.com

e24cloud rozesłał swoim klientom następującą wyjaśnienia:

(…) Przyczyną przerwy w dostępności zasilania był fatalny zbieg okoliczności – nałożenie się sytuacji awaryjnych w kluczowych punktach instalacji:

a. awaria układu automatycznego sterowania rozdzielniami elektrycznymi,

b. awaria jednego z głównych wyłączników układu SZR,

c. nieprecyzyjne dane na temat czasu pracy na bateriach – urządzenia podają 25 minut podczas kiedy faktycznie ten czas jest krótszy (15min).

Dodatkowym okolicznością, która wpłynęła na przebieg awarii był tzw. czynnik ludzki – tak skomplikowany przebieg awarii zwiększył poziom stresu, co negatywnie wpłynęło na szybkość podejmowania decyzji. (…)

Case Study awarii e24cloud.com

e24cloud posiada certyfikat zgodność z TIER

TIER2	TIER3	TIER4
Medium-size Businesses	Large Businesses	Enterprise Corporations
99.749% Uptime	99.982% Uptime	99.995% Uptime
22 Hours	1.6 Hours	2.4 Minutes
Downtime Per Year	Downtime Per Year	Downtime Per Year
Partial Redundancy in Power and Cooling	N+1 Fault Tolerant	2N+1 Fully Redundant
	72 Hour Power Outage Protection	96 Hour Power Outage Protection

Case Study awarii e24cloud.com

Zostałeś poszkodowany w awarii e24cloud.com? Dostaniesz rabat!

2. Promocja skierowana jest do wszystkich osób, które potrafią udokumentować, że w czasie trzech miesięcy wstecz od dn 04.06.2012 roku korzystały z usług ecloud24.com, np okazując kopię faktur za usługę, lub też umowy z ecloud24.com zawartej

5. W ramach promocji Firma X udzieli rabatu w wysokości 30% na wszystkie usługi wymienione w punkcie 3 dla osób które spełniają założenia punktu 2 na okres jednego roku od dnia zawarcia umowy. Promocją nie są objęte usługi dodatkowe dedykowane dla usług wymienionych w punkcie 3.

Na początku było słowo/pytanie

Jaki jest akceptowalny
czas przestoju
systemów informatycznych naszej firmy

w omawianym Case Study odtwarzanie dostępności usług trwało ponad 2 dni ☹

Case Study awarii e24cloud.com

Wnioski

1) Korzystanie z Cloud Computing **nie daje** 99,9% pewności zapewnienia ciągłości działania

2) Korzystanie z Cloud Computing **nie daje** 99,9% pewności poprawnego Disaster Recovery

3) Nacisk na ekonomię rozwiązań Cloud Computing może spowodować wpadnięcie w pułapkę najniższej ceny za najniższą jakość usług

4) Ryzyka związane z „technikaliami” to tylko wierzchołek góry lodowej ryzyk związanych z Cloud Computing

Inne głośne awarie:

1) Awaria BlackBerry uderzyła w cztery kontynenty - miliony klientów biznesowych na kilku kontynentach bez dostępu do mobilnej poczty elektronicznej,

2) VMware: druga awaria Cloud Foundry efektem błędu w czasie naprawy pierwszej

3) Połowa Internetu nie działa - awaria chmury Amazon EC2 (Elastic Compute Cloud)

Ryzyka związane z Cloud Computing

1) Ryzyka Dostępności
2) Ryzyka Bezpieczeństwa
3) Ryzyka Zgodności
4) Ryzyka Prawne

Ryzyka Bezpieczeństwa związane z Cloud Computing

Dane w modelu tradycyjnym stanowią własność klienta i są wewnętrznie zarządzane przez jego własne zasoby.

W momencie przejścia na usługę cloud computing w pierwszej kolejności należy formalnie określić właścicielstwo danych. **Wbrew pozorom nie jest to oczywiste że właścicielem danych jest usługobiorca** .

W modelu Cloud Computing należy zapewnić odpowiednią poufność oraz integralność danych. Współdzielenie zasobów, które jest cechą charakterystyczną Cloud Computing w praktyce oznacza, że z tej samej aplikacji (ale różnych jej instancji) korzysta równolegle wielu klientów usługi.

Ryzyka Bezpieczeństwa związane z Cloud Computing

Podatności w aplikacji mogą spowodować, że zabezpieczenia separujące poszczególnych klientów zawiodą. W tym momencie narażamy się na ujawnienie wewnętrznych danych osobom postronnym. Ponadto dostęp do danych jest teoretycznie możliwy przez samego usługodawcę Cloud Computing.

Stosowanie mechanizmów kryptograficznych może stanowić racjonalne zabezpieczenie przed tym ryzykiem.

Bezpieczne usuwanie danych - uprzednio skasowane dane firmy są w dalszym ciągu przechowywane w chmurze bez wiedzy firmy

Ryzyka Bezpieczeństwa związane z Cloud Computing

Opinia Grupy Roboczej Art. 29 (od nr art. 29 Dyrektywy 95/46/WE) w sprawie przetwarzania danych w chmurze obliczeniowej, 1.07.2012 r.

http://www.giodo.gov.pl/259/id_art/4815/j/pl

Mimo uznanych korzyści płynących z przetwarzania danych w chmurze (tzw. Cloud Computingu) zarówno pod względem ekonomicznym, jak i społecznym, w niniejszej opinii przedstawiono, w jaki sposób wykorzystanie usług przetwarzania w chmurze na szeroką skalę może wywołać szereg zagrożeń, głównie takich jak brak kontroli nad danymi osobowymi oraz niewystarczające informacje na temat tego, w jaki sposób, gdzie i przez kogo dane są przetwarzane / przetwarzane przez podmiot, któremu powierzono przetwarzanie. Organy publiczne i przedsiębiorstwa prywatne muszą dokładnie ocenić te zagrożenia, gdy rozważają skorzystanie z usług oferowanych przez dostawcę usług w chmurze.

Ryzyka Zgodności związane z Cloud Computing

Badanie ryzyka zgodności (standardów) powinno zawierać również analizę związaną z kosztami zmiany usługodawcy taka by nie doszło do tzw. vendor -lock-in uzależnienia się od usługodawcy.

Próba uzyskania przez usługodawców przewagi konkurencyjnej – ryzykiem odbiorcy.

Nad kwestiami związanymi ze zgodnością 27.09.2012 pochyliła się Komisja Europejska określając strategię dotyczącą Cloud Computing. Mają to być działania zmierzające do uzyskania takich korzyści z chmur, jak 2,5 mln nowych miejsc pracy w Europie oraz roczny przyrost PKB UE na poziomie 160 mld EUR (ok. 1%) do 2020 r.

Ryzyka Zgodności związane z Cloud Computing

Główne działania założone w strategii to:

Rozwiązanie problemu mnogości standardów, aby zapewnić użytkownikom chmury interoperacyjność, przenoszenie danych i odwracalność danych. Niezbędne normy mają być określone do 2013 r.

Promowanie ogólnounijnych mechanizmów certyfikacji dla wiarygodnych dostawców usług w modelu chmury.

Opracowanie wzoru "bezpiecznych i uczciwych" warunków dla umów dotyczących usług w chmurze, w tym umów o gwarantowanym poziomie usług.

Ustanowienie europejskiego partnerstwa na rzecz chmur obliczeniowych.

http://www.scribd.com/doc/107144037/Komunikat-KE

Ryzyka Prawne związane z Cloud Computing

Brak definicji Cloud Computing w prawie polskim (dobrze czy źle ?)

Prawa autorskie - Umowy licencyjne na programy operacyjne, bądź aplikacje mogą zawierać postanowienia uniemożliwiające korzystanie z nich w chmurze lub wprowadzać istotne ograniczenia. W przypadku naruszenia praw autorskich, uprawniony może dochodzić odszkodowania od wszystkich korzystających, tj. zarówno od usługodawcy, jak i usługobiorcy.

Mimo wspólnych unijnych ram prawnych brak dostatecznej harmonizacji obowiązujących w poszczególnych państwach członkowskich przepisów o ochronie danych

Ryzyka Prawne związane z Cloud Computing

„Miejsce” przetwarzania danych w modelu Cloud Computing.

Dyrektywa Parlamentu Europejskiego z dnia 24 października 1995 w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych.

Według Dyrektywy, gdy administrator danych i przetwarzający dane znajdują się w różnych Państwach EOG, relacją między administratorem danych i przetwarzającym rządzi prawo ochrony danych osobowych państwa siedziby administratora danych. Dodatkowo do przetwarzającego dane stosują się zasady zabezpieczenia danych osobowych określone w państwie siedziby przetwarzającego.

Ryzyka Prawne związane z Cloud Computing

Realizacja wymogów dotyczących przetwarzania danych osobowych - ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U.02.101.926).

UODO nakazuje, aby powierzenie przetwarzania danych osobowych przetwarzającemu przez administratora danych nastąpiło na podstawie umowy o powierzenie przetwarzania danych osobowych. Przepis UODO stanowi, że umowa taka powinna być zawarta w formie pisemnej.

Brak formy pisemnej może rodzić negatywne konsekwencje dla administratora danych na gruncie prawa administracyjnego, GIODO może wydać decyzję nakazująca zawarcie takiej umowy w formie pisemnej. **Teoretycznie może też skutkować odpowiedzialnością karną za nienależyte zabezpieczenie danych osobowych.**

Ryzyka Prawne związane z Cloud Computing

Art. 31. 1. Administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych.

2. Podmiot, o którym mowa w ust. 1, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

3. Podmiot, o którym mowa w ust. 1, jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36-39, oraz spełnić wymagania określone w przepisach, o których mowa w art. 39a. W zakresie przestrzegania tych przepisów podmiot ponosi odpowiedzialność jak administrator danych.

4. W przypadkach, o których mowa w ust. 1-3, odpowiedzialność za przestrzeganie przepisów niniejszej ustawy spoczywa na administratorze danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową.

Ryzyka Prawne związane z Cloud Computing

Uwagi Grupy Roboczej Art. 29

1. Brak poufności w odniesieniu do wniosków z zakresu egzekwowania prawa składanych bezpośrednio do dostawcy usługi w chmurze: dane osobowe przetwarzane w chmurze mogą być przedmiotem wniosków z zakresu egzekwowania prawa pochodzących od organów egzekwowania prawa z państw członkowskich UE oraz krajów trzecich. **Istnieje zagrożenie, że dane osobowe mogłyby być ujawnione (zagranicznym) organom egzekwowania prawa bez ważnej podstawy prawnej UE i tym samym doszłoby do naruszenia prawa UE dotyczącego ochrony danych.**
2. Brak możliwości interwencji ze względu na złożoność i dynamiczność łańcucha outsourcingu: Usługa w chmurze oferowana przez jednego dostawcę może być realizowana poprzez połączenie usług od szeregu innych dostawców, które mogą być dynamicznie dodawane lub usuwane w czasie trwania umowy klienta.

Ryzyka Prawne związane z Cloud Computing

Uwagi Grupy Roboczej Art. 29

3. Brak możliwości interwencji (prawa osób, których dane dotyczą): Dostawca usługi w chmurze może nie zapewnić niezbędnych środków i narzędzi mających pomóc administratorowi zarządzać danymi np. w zakresie dostępu, usunięcia lub poprawienia danych.
4. Brak odizolowania: Dostawca usługi w chmurze może wykorzystywać swoją fizyczną kontrolę nad danymi od różnych klientów w celu łączenia danych. Jeżeli dostawcy usługi administrujący przetwarzaniem mieliby wystarczające prawa uprzywilejowanego dostępu (role wysokiego ryzyka), mogliby łączyć informacje od różnych klientów (administratorów danych).

Wnioski

Najważniejsze są nie „technikalia” i kwestie wydajnościowe lecz zapisy w umowie:

Zapisy w umowie – rekomendacje Grupy Roboczej Art. 29

1) Określenie środków bezpieczeństwa, z którymi dostawca usługi w chmurze musi zapewnić zgodność, w zależności od zagrożeń związanych z przetwarzaniem i charakterem danych, które mają być chronione.

2) Przedmiot i ramy czasowe usługi w chmurze, która ma być świadczona przez dostawcę usługi w chmurze, zakres, sposób i cel przetwarzania danych osobowych przez dostawcę usługi w chmurze, jak również rodzaje przetwarzanych danych osobowych.

3) Określenie warunków zwrotu danych (osobowych) lub zniszczenia danych po zakończeniu realizacji usługi. Ponadto należy zapewnić, aby dane osobowe usunąć bezpiecznie na wniosek klienta usługi w chmurze.

4) **Zawarcie klauzuli poufności, wiążącej zarówno dostawcę usługi w chmurze, jak i wszelkich jego pracowników, które mogą mieć możliwość dostępu do danych. Tylko upoważnione osoby mogą mieć dostęp danych.**

Zapisy w umowie – rekomendacje Grupy Roboczej Art. 29

5) Obowiązek po stronie dostawcy do wspierania klienta w ułatwianiu realizacji praw osoby, której dane dotyczą, do dostępu do swoich danych, ich poprawienia lub usunięcia.

6) Wyjaśnienie zobowiązań dostawcy usługi w chmurze dotyczących zawiadamiania klienta usługi w chmurze w przypadku wszelkich naruszeń ochrony danych, które mają wpływ na dane klienta usługi w chmurze.

7) Obowiązek dostawcy usługi w chmurze dotyczący wskazania listy lokalizacji, w których dane mogą być przetwarzane.

8) Należy określić w umowie, że dostawca usługi w chmurze musi poinformować klienta o istotnych zmianach dotyczących określonej usługi w chmurze, takich jak wdrożenie dodatkowych funkcji.

Zapisy w umowie – rekomendacje Grupy Roboczej Art. 29

Należy zauważyć, że w wielu przypadkach dostawcy usług w chmurze oferują standardowe usługi i umowy, które mają być podpisane przez administratorów, które przewidują standardową formę przetwarzania danych osobowych. **Ten brak równowagi w uprawnieniach umownych małego administratora w odniesieniu do dużych dostawców usług nie może być uznany za usprawiedliwienie dla administratorów** do przyjęcia klauzul i warunków umowy, które nie są zgodnie z prawem dotyczącym ochrony danych.

Artykuł 17 ust. 2 dyrektywy 95/46/WE **nakłada na klientów usług w chmurze (działających jako administratorzy danych) pełną odpowiedzialność za wybranie dostawców usług w chmurze**, którzy wdrożą odpowiednie techniczne i organizacyjne środki bezpieczeństwa w celu ochrony danych osobowych oraz w celu możliwości wykazania rozliczalności.

Powszechna praktyką jest zawieranie umów SLA z dostawcami usług Cloud Computing. Oprócz samego zawarcia umowy, należy pamiętać, że po stronie usługobiorcy jest monitorowanie zgodności dostawcy z SLA.

Pytanie

Czy posiadamy w naszej organizacji niezbędne zasoby kompetencyjne aby monitorować jakość deklarowanych/oferowanych usług ?

Rozwiązanie

- ✓ Audytorzy ISACA – www.isaca.katowice.pl
- ✓ Rzeczoznawcy Izby Rzeczoznawców Polskiego Towarzystwa Informatycznego http://www.pti.org.pl/index.php/corporate/Uslugi-profesjonalne/Izba-Rzeczoznawcow-PTI
- ✓ Specjaliści Cloud Security Alliance – Certificate of Cloud Security Knowledge (CCSK)

Rekomendacja „D" Komisji Nadzoru Finansowego

W dniu 8 stycznia 2013 r. KNF jednogłośnie przyjęła **Rekomendację D** dotyczącą zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach.

W przypadku, gdy usługi świadczone przez podmiot zewnętrzny obejmują przetwarzanie danych o wysokim stopniu poufności lub istotności dla banku41 poza infrastrukturą teleinformatyczną banku (np. w modelu *Cloud Computing* lub innych formach modelu *Application Service Provision*, w zewnętrznych centrach przetwarzania danych itp.), bank powinien w szczególności:

- ✓ wprowadzić odpowiednie mechanizmy kontrolne zapewniające poufność tych danych (np. poprzez ich szyfrowanie),
- ✓ **zapewnić, aby informacje o wszelkich incydentach zagrażających bezpieczeństwu danych były raportowane przez dostawcę,**

Rekomendacja „D” Komisji Nadzoru Finansowego

- ✓ posiadać informacje o tym, w jakich lokalizacjach geograficznych dane te są przetwarzane oraz jakie przepisy prawa obowiązują tam w przedmiotowym zakresie, oraz zapewnić zgodność świadczonych usług z przepisami prawa obowiązującymi w Polsce,

- ✓ **zapewnić skuteczne mechanizmy pozwalające na bezpieczne zakończenie współpracy (w szczególności w zakresie zwrotu danych oraz ich usunięcia – wraz ze wszystkimi kopiami – przez dostawcę usług),**

- ✓ przeanalizować zasadność i na tej podstawie podjąć odpowiednią decyzję dotyczącą wprowadzenia obowiązku przedstawiania przez dostawcę certyfikatów w zakresie zgodności z uznanymi międzynarodowymi normami dotyczącymi bezpieczeństwa informacji (szczególnie w przypadku przetwarzania danych poza granicami Europejskiego Obszaru Gospodarczego).

Raport „HP Research: The Future of Cloud”

- ✓ Obecnie tylko 24% modeli świadczenia usług w przedsiębiorstwach opiera się na chmurach obliczeniowych. Dyrektorzy ds. biznesowych i technicznych szacują, że do 2020 r. liczba modeli publicznych i prywatnych chmur obliczeniowych ulegnie niemal podwojeniu.

- ✓ Najważniejsze czynniki przemawiające za wdrożeniem przetwarzania w chmurze to szybkie opracowywanie aplikacji (50%), większa elastyczność reakcji na zmiany rynkowe (32%) i niższe koszty operacyjne (18%).

- ✓ Ankietowani dyrektorzy ds. biznesowych i informatycznych podkreślają, że wdrożenia przetwarzania w chmurze będą miały kluczowe znaczenie dla zapewnienia dobrych wyników i wprowadzania innowacji. **Mniej więcej co drugi dyrektor generalny i dyrektor ds. finansowych przygotowuje właśnie strategię wdrożenia chmury w swoim przedsiębiorstwie.**

Konkludując – co począć z Cloud Computing ?

1) Inwentaryzacja / aktualizacja katalogu usług IT biznesowych zgodnie z ITIL

2) Ocena poziomu istotności dla organizacji poszczególnych usług IT biznesowych

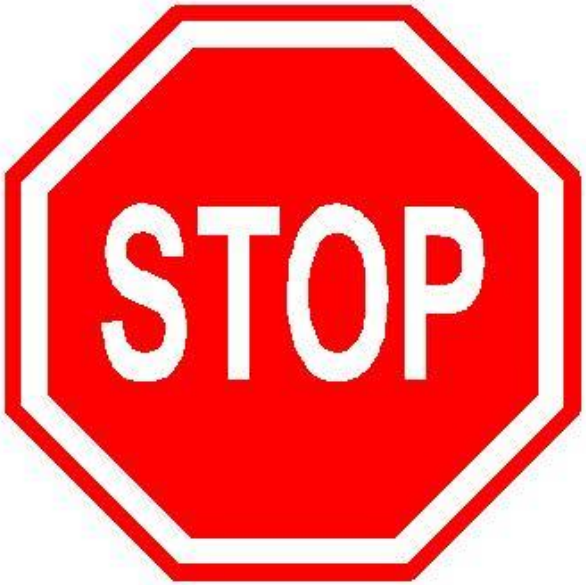
3) Wycena kosztów poszczególnych usług IT biznesowych

4) Analiza SWOT migracji do Cloud Computing poszczególnych usług IT biznesowych – w szczególności w kontekście ryzyk

5) Szukajmy dostawców z indywidualnym podejściem do klienta

PYTANIA ?

PYTANIA ?



NIE

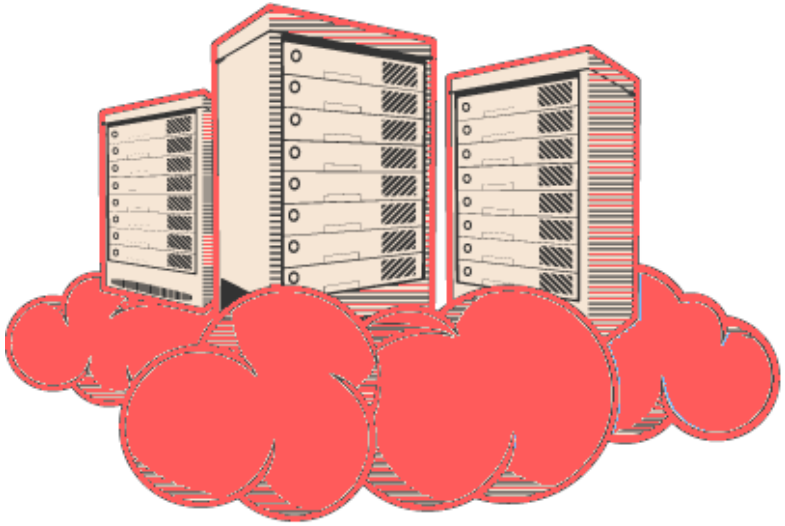
PROSZĘ

O

DYSKUSJĘ !!!

ISACA
Trust in, and value from, information systems
Katowice Chapter

DZIĘKUJE ZA UWAGĘ



Adam Mizerski adam@mizerski.net.pl 507-071-401