Robert Michalski
Security Tiger Team

Bezpieczeństwo w chmurze – nie taki wilk straszny jak go malują!

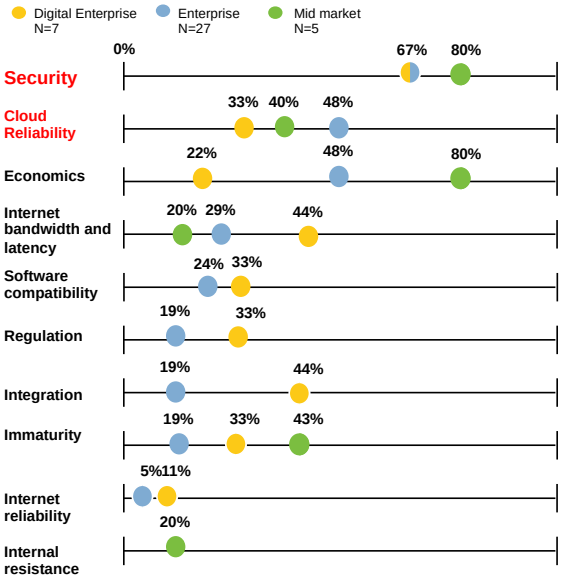
V Zachodniopomorski Konwent Informatyków

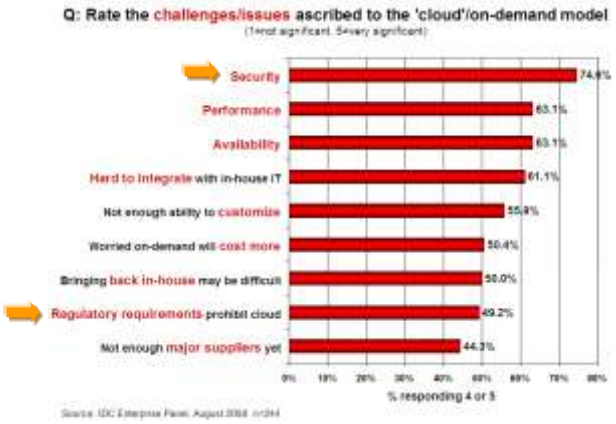
15.09.2011 Międzywodzie

Agenda

1. Trochę kłamstw..
2. Chmura kątem oka „bezpiecznika”
3. Punkt widzenia IBM
4. Czy w chmurze może być bezpieczniej?

62% organizacji ma bardzo małą lub zerową pewność, że może zabezpieczyć zasoby działające w chmurze. Wśród 49% respondentów, którzy rozpoczęli działanie w chmurze ponad 1/3 (39%) ma poważne zastrzeżenia związane z bezpieczeństwem.



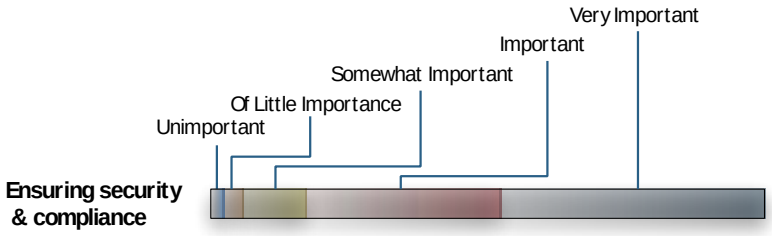


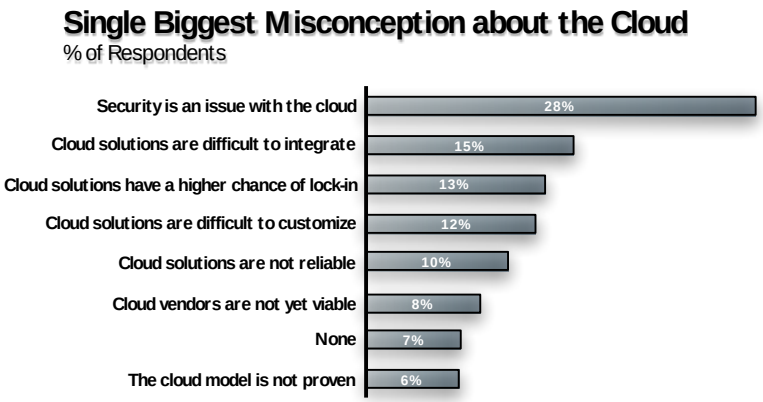
Source: Oliver Wyman Interviews

Dlaczego chmura jest ciężka do zaakceptowania?

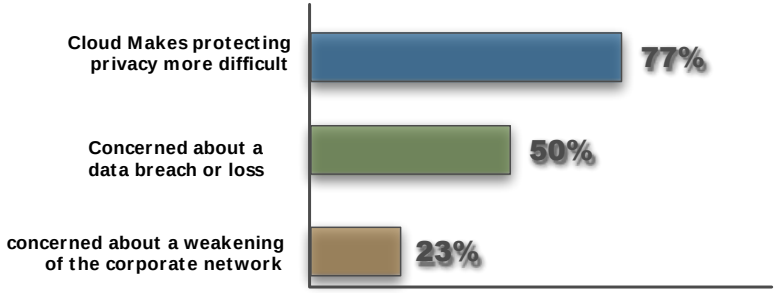
Bezpieczeństwo w chmurze

Wg badań przeprowadzonych przez Appirio na ponad 150 średnich i dużych firmach po adaptacji chmury:





Badania przeprowadzone przez IBM w ramach 2010 Global IT Risk Study pokazują, że przetwarzanie w chmurze wywołuje poważne obawy o użycie, dostęp i kontrolę danych.



Czym jest Cloud Security?

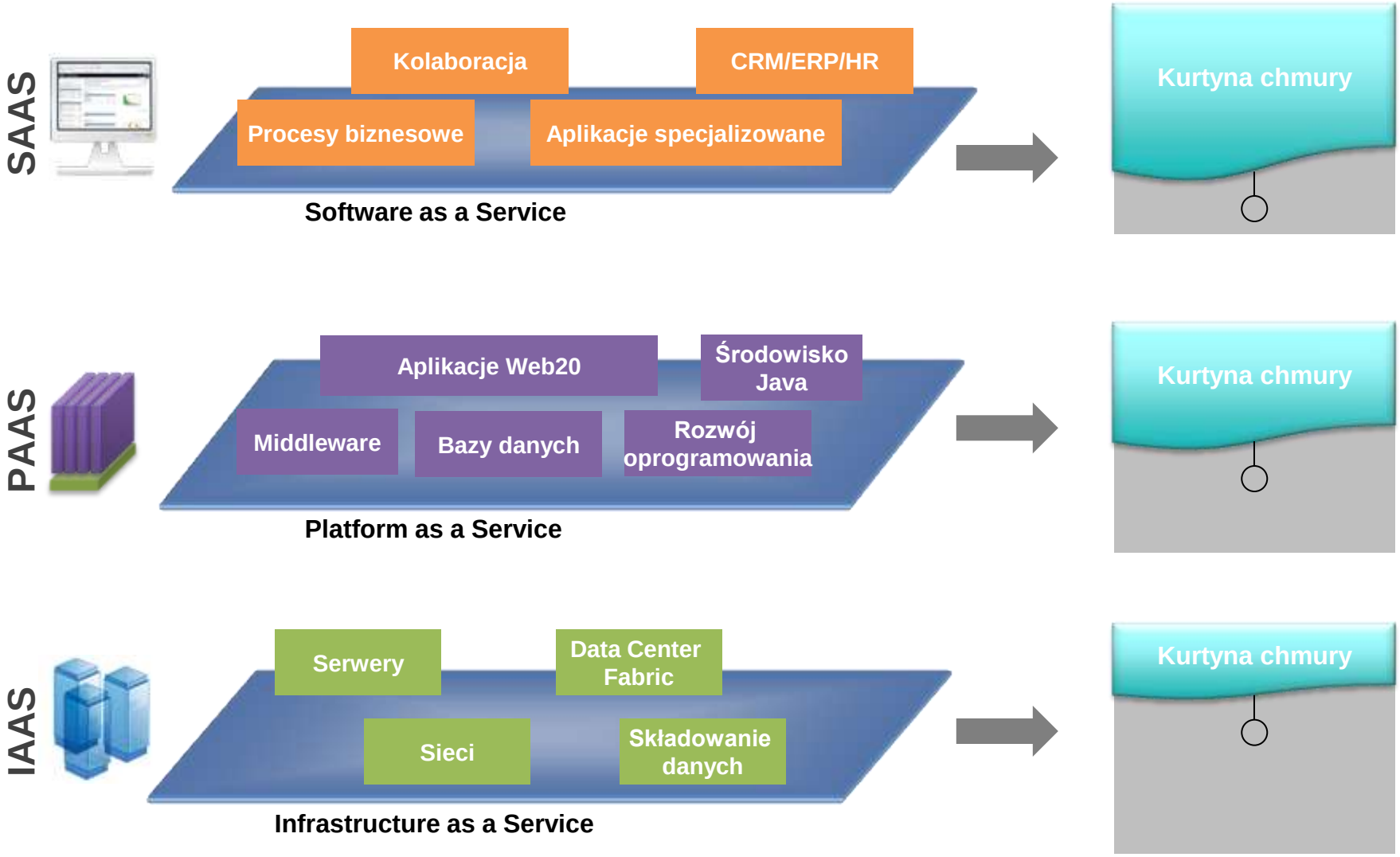
Poufność, integralność i dostępność krytycznych zasobów IT

Te same potrzeby, nowe wyzwania

Nie ma nic nowego pod słońcem, ale jest jeszcze mnóstwo rzeczy o których nic nie wiemy.

Ambrose Bierce, Słownik diabła

Różne chmury, różne wyzwania



Kategorie ryzyk związanych z przetwarzaniem w chmurze

Kontrola

Wiele organizacji czuje się niekomfortowo wiedząc, że ich dane są zlokalizowane w systemach, których nie kontrolują

Dane

Migracja przetwarzania do wspólnej infrastruktury zwiększa ryzyko nieautoryzowanego dostępu.

Niezawodność

Wysoka dostępność jest kwestią kluczową. Działy IT obawiają się niedostępności serwisów w przypadku awarii.

Regulacje

Zgodność z PCI, SOX i innymi regulacjami może skutecznie blokować zastosowanie chmur.

Zarządzanie bezpieczeństwem

Brak przejrzystości w warstwie abstrakcji chmury.

Typowe wymagania bezpieczeństwa wobec chmury*

Nadzór IT, Zarządzanie ryzykiem, Regulacje

- **Zewnętrzny audyt** (SAS 70(2), ISO27001, PCI)
- **Dostęp klienta do dotyczących go logów i danych audytowych**
- **Efektywne raportowanie incydentów per klient**
- Wgląd w zarządzanie zmianą, incydentami, obrazami
- SLA, opcja transferu ryzyka z najemcy na dostawcę
- Wsparcie analizy powłamaniowej

Aplikacje i procesy

- Bezpieczeństwo aplikacji jest podnoszone na równi z bezpieczeństwem wirtualnych obrazów
- Zgodność z dobrymi praktykami w zakresie rozwoju oprogramowania

Warstwa fizyczna

- Monitorowanie i kontrola fizycznego dostępu

Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security;

IBM RedGuide REDP-4528-00, July 2009

Ludzie i tożsamość

- **Monitorowanie użytkowników uprzywilejowanych,** włączając logowanie aktywności, fizyczny monitoring i sprawdzenie reputacji
- **Federacyjność:** Uwierzytelnieanie i autoryzacja w rozproszonym środowisku
- **Bazujące na standardach SSO**

Dane i informacje

- **Segregacja danych**
- Kontrola klienta nad geograficzną lokalizacją danych
- Sektor publiczny: klasyfikacja danych

Sieć, serwer, stacja końcowa

- **Izolacja** między domenami najemców
- **Granulacja wirtualnych domen:** możliwość kontroli bezpieczeństwa w polityce per strefa
- Wbudowana detekcja i zapobieganie włamaniom
- Zarządzanie podatnościami
- Ochrona obrazów wirtualnych maszyn przed uszkodzeniem i nadużyciami
- Sektor publiczny: wysoce kontrolowana seperacja

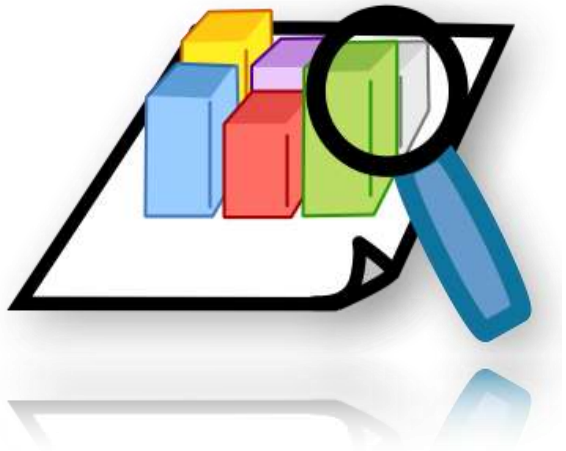
**Bazuje na wywiadach z klientami i opiniach analityków*

Infrastruktura w chmurze

- Na poziomie sieciowym
  - Używanie do transmisji do chmury i z chmury otwartych protokołów (bez szyfrowania)
  - Możliwe błędy w konfiguracji kluczowych aspektów warstwy sieciowej – np. BGP-prefix
  - Problemy z DNS, osłabiony „split-horizon”, stare ataki typu cache-poisoning, czy bugi ala Dan Kaminsky
  - Separacja na poziomie domeny zamiast stref i wartstw
- Na poziomie hosta
  - Bezpieczeństwo systemu wirtulizacyjnego – system zarządzania, hypervisor, VMEscape, VMtakeover, VMsprawl
  - Dynamiczność środowiska – przenoszenie maszyn między fizycznymi maszynami na gorąco a polityka bezpieczeństwa, snapshoty a łatanie czy aktualność innych mechanizmów bezpieczeństwa jak antywirus
  - Słabo zabezpieczone obrazy startowe – niepotrzebne usługi, brak mechanizmów bezpieczeństwa czy brak logowania

Aplikacje w chmurze

- Brak praktyk rozwoju i życia oprogramowania (SDLC), co zwłaszcza w kontekście aplikacji webowych może grozić poważnymi konsekwencjami np.. XSS, SQL Injection
- Poleganie na warstwie sieci i hosta w zakresie ochrony aplikacji, brak dedykowanych mechanizmów np. WAF, SOA Security
- Ataki odmowa usługi (DoS) na aplikacje np. duża ilość zapytań XML-owych via HTTPS nastawione na wysycenie zasobów
- Ataki ekonomiczne (EDoS) nastawione na obciążenie organizacji kosztami przetwarzania, bądź zablokowanie usługi na skutek wyczerpania zasobu



Dane w chmurze

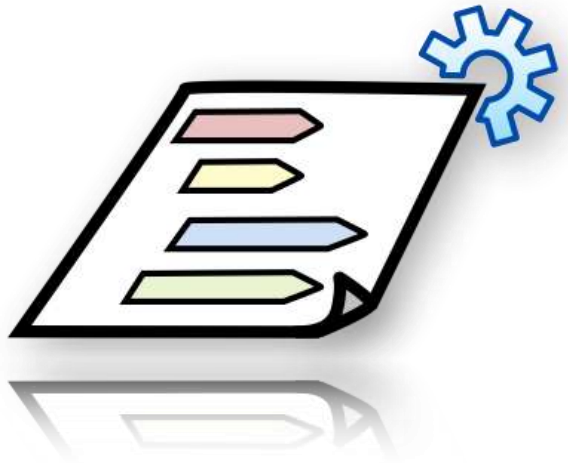
- Brak mechanizmów zapewnienia poufności danych w chmurze w zakresie transmisji, przechowywania i przetwarzania lub ich zła konfiguracja np. jeden klucz szyfrowania danych dla wszystkich klientów chmury, słaby lub nieistniejący proces zarządzania kluczami szyfrowania
- Brak izolacji danych lub słabe mechanizmy izolacji np. poleganie na aplikacji w zakresie zapewnienia izolacji na podstawie tagowania
- Granulacja kontroli dostępu – z reguły zbyt szerokie uprawnienia
- Brak lub słabe gwarancje dostępności danych

Tożsamość w chmurze

- Jeden z kluczowych elementów który zdecyduje o powodzeniu przetwarzania w chmurze!
- Przestrzeń zarządzania tożsamością, w tym kontrolą dostępu to dwukierunkowa ulica – z jednej strony liczy się otwartość dostawcy w zakresie standardów i elastyczność konfiguracji, a z drugiej gotowość informatyczna najemcy
- Wsparcie federacyjności – SAML, WS-*, Liberty Alliance
- Ryzyka, które w tym obszarze występują nie różnią się znacząco od tych z którymi mamy do czynienia w tradycyjnym środowisku

Regulacje i prywatność w chmurze

- Zapewnienie zgodności z regulacjami zewnętrznymi jest w wielu przypadkach blokadą w przejściu do publicznej chmury
- Przykładem problematyczności niektórych zapisów w standardach niech będzie wymaganie: pojedyncza funkcja per serwer ze standardu PCI DSS
- O ile przetwarzanie meta-danych zwykle nie jest problematyczne z punktu widzenia regulacji dotyczących choćby danych personalnych to już same dane podlegają bardzo ścisłym rygorom – np. nie mogą opuszczać kraju pochodzenia bądź określonej strefy np. UE
- Nawet jeśli uda się spełnić wymagania dotyczące bezpieczeństwa samych danych to może się okazać, że dostawca nie będzie w stanie spełnić wymagań w zakresie kontroli nadzoru IT



Zaufany doradca | Dostawca rozwiązań | Producent bezpieczeństwa | Firma z tradycją

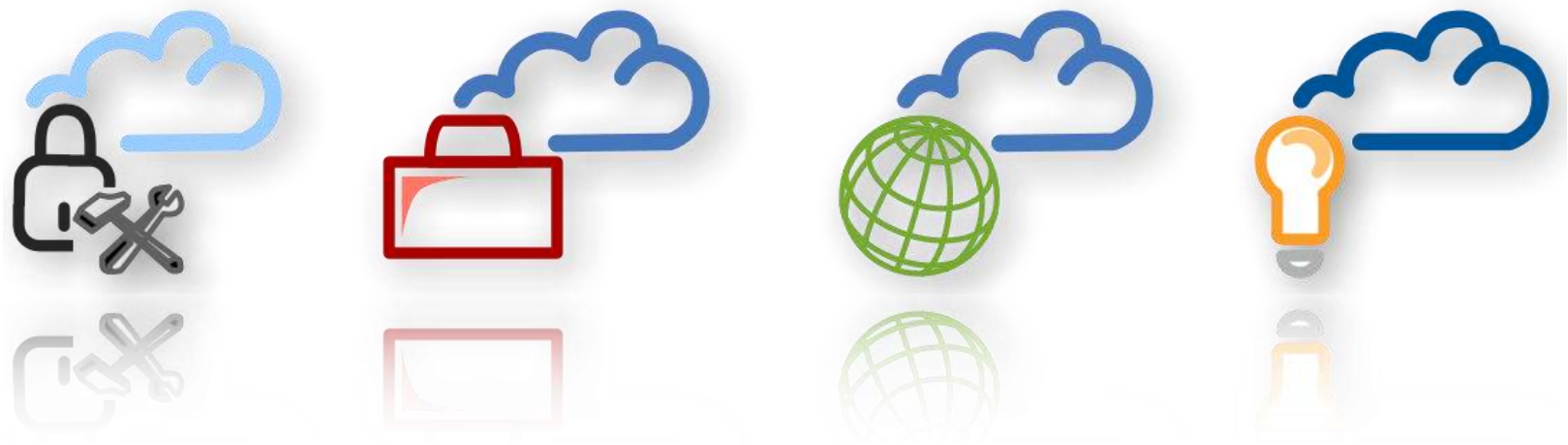
Bezpieczeństwo chmury | **Bezpieczeństwo z chmury**

Podejście IBM do bezpieczeństwa w chmurze

IBM rozumie chmurę i rozumie też, że

“Jeden rozmiar nie dla wszystkich”

Jak IBM patrzy na chmurę?



Bezpieczeństwo „wbudowane”

Bezpieczeństwo zależne od typu przetwarzania

Bezpieczeństwo mierzalne

Bezpieczeństwo innowacyjne

Przewodnik IBM po bezpieczeństwie przetwarzania w chmurze

Bazuje na wewnętrznej szerokiej dyskusji w IBM i interakcji z klientami

Uwypukla najlepsze praktyki, które powinny zostać zaimplementowane

Składa się z 7 komponentów:

- Budowa programu bezpieczeństwa
- Ochrona danych poufnych
- Implementacja silnych mechanizmów kontroli dostępu i tożsamości
- Aprowizacja i de-aprowizacja aplikacji
- Zarządzanie audytem i nadzorem IT
- Zarządzanie podatnościami
- Testowanie i walidacja


IBM

Redpaper

Axel Buecker
Kaos Lodewijkx
Harold Moss
Kevin Skapinetz
Michael Waidner

Cloud Security Guidance

IBM Recommendations for the Implementation of Cloud Security

In this IBM® Redpaper™ publication, we provide a discussion about the IBM recommendations for the implementation of cloud security. To get started, let us begin with an introduction to cloud computing and cloud security in general.

Introduction to cloud computing

Cloud computing is a flexible, cost-effective, and proven delivery platform for providing business or consumer IT services over the Internet. Cloud resources can be rapidly deployed and easily scaled, with all processes, applications, and services provisioned *on demand*, regardless of the user location or device.

As a result, cloud computing gives organizations the opportunity to increase their service delivery efficiencies, streamline IT management, and better align IT services with dynamic business requirements. In many ways, cloud computing offers the *best of both worlds*, providing solid support for core business functions along with the capacity to develop new and innovative services.

Note: As an added benefit, cloud computing enhances the user experience without adding to its complexity. Users do not need to know anything about the underlying technology or implementations.

Both public and private cloud models are now in use. Available to anyone with Internet access, public models include *Software as a Service* (SaaS) clouds, such as IBM LotusLive, *Platform as a Service* (PaaS) clouds, such as Amazon Web Services, and *Security and Data Protection as a Service* (SDPaaS) clouds, such as IBM Security Event and Log Management Services.

Private clouds are owned and used by a single organization. They offer many of the same benefits as public clouds, and they give the owner organization greater flexibility and control.

© Copyright IBM Corp. 2009. All rights reserved. ibm.com/redbooks 1

http://www.redbooks.ibm.com/abstracts/redp4614.html?Open

Chmura daje możliwość zwiększenia bezpieczeństwa!

	Kontrola w chmurze	Korzyść
Ludzie i tożsamość	•Zdefiniowany zestaw interfejsów •Centralne repozytorium tożsamości i polityk kontroli dostępu	•Zmniejszone ryzyko niepowołanego dostępu do danych
Informacje i dane	•Zasoby obliczeniowe w izolowanych domenach określonych w katalogach usług •Domyślne szyfrowanie danych w ruchu i spoczynku •Zapewnienie lepszego przechowywania wirtualnych zasobów, kontrola i śledzenie danych	•Poprawienie rozliczalności. Zmniejszenie ryzyka wycieku danych. •Zmniejszona powierzchnia ataków •Mniejsze prawdopodobieństwo propagacji ataku
Procesy i aplikacje	•Autonomiczne polityki bezpieczeństwa •Personel i narzędzia specjalizowane do ekosystemu chmury •SLA na dostępność i poufność	•Lepsza ochrona aktywów i zwiększenie rozliczalności biznesu i użytkowników IT
Sieć, serwer i stacja końcowa	• Automatyczna aprowizacja utwardzonych obrazów systemowych •Dynamiczna alokacja zasobów ukierunkowana na realizację konkretnego zadania	•Zmniejszona powierzchnia ataków •Wieksze możliwości analizy powłamaniowej dzięki snapshotom
Fizyczna infrastruktura	•Zwiększone sprzężenie systemów do zarządzania fizycznym i logicznym dostępem.	•Ulepszone możliwości egzekwowania reguł dostępu i zarządzania zgodnością

To co jest potencjalną słabością chmury może być jej siłą!

- Nie ma nic nowego pod słońcem, obawiamy się tego czego nie znamy
- Nie ma jednej chmury dla wszystkich, specjalizacja pożądana
- Chmura szansą na zwiększenie i uproszczenie bezpieczeństwa
- Chmura szansą na innowacje w bezpieczeństwie

IBM.COM/SECURITY

ROBERT.MICHALSKI@PL.IBM.COM

TEL. +48 693-93-5737

IBM Security Solutions

Funkcja	Rozwiązanie z portfolio IBM
1. Budowa infrastruktury chmurowej:	• IBM Tivoli Service Automation Manager • IBM Tivoli Monitoring • IBM Service Delivery Manager • IBM Cloud Architecture / Design Services
2. Ustanowienie i egzekucja polityki bezpieczeństwa oraz struktury nadzoru	• IBM Professional Security Services • IBM Tivoli Security Policy Manager • IBM Websphere Datapower SOA Appliance • IBM Tivoli Security Incident & Event Manager • IBM InfoSphere Guardium
3. Wykrywanie i kategoryzacja zasobów informacyjnych	• IBM InfoSphere Optim • IBM InfoSphere Guardium
4. Ustanowienie i zarządzanie tożsamościami i dostępem	• IBM Tivoli Identity Manager • IBM Tivoli Access Manager • IBM Tivoli Federated Identity Manager • IBM Tivoli Security Incident & Event Manager • IBM Privileged Identity Management
5. Zarządzanie dostępem do informacji	• IBM InfoSphere Guardium

IBM Security Solutions

Funkcja	Rozwiązanie z portfolio IBM
6. Ochrona przed zagrożeniami	• IBM AppScan • IBM Managed Security Services • IBM Proventia Threat Mitigation Products • IBM Tivoli Endpoint Manager (BigFix) • IBM Security Virtual Server Protection • IBM X-Force Threat Analysis Service (XFTAS)
7. Bezpieczeństwo fizyczne	• IBM Physical Security Services – Digital Video Surveillance
8.Bieżący widok w środowisko i raportowanie zgodności z regulacjami	• IBM Tivoli Security Incident & Event Manager • IBM InfoSphere Guardium • IBM Tivoli Monitoring • IBM Proventia Management SiteProtector • IBM Tivoli Netcool OMNIbus
9. Zaawansowana analityka / Wykrywanie i reagowanie na incydenty	• IBM Research • IBM InfoSphere Streams • IBM CognosNow • IBM Tivoli Service Automation Manager • IBM Service Delivery Manager