Bezpieczeństwo chmury – szansa czy zagrożenie dla Banków Spółdzielczych?

Aleksander P. Czarnowski

AVET Information and Network Security Sp. z o.o.

AVET
Information and Network Security

Agenda

- Cloud Computing – definicja
- Modele biznesowe
- Zagrożenia
- Dlaczego tworzyć bezpieczne chmury w Bankowości Spółdzielczej?
- Jak stworzyć bezpieczną chmurę w Banku Spółdzielczym?
- Pytania

Model rozproszonego przetwarzania oparty na użytkowaniu usług dostarczonych przez zewnętrzne lub wewnętrzne organizacje.

***CLOUD COMPUTING* = PRZETWARZANIE W CHMURZE**

Cloud Computing - definicja

- Podstawowe rodzaje chmur:
  - ***Publiczna*** – udostępniana przez zewnętrznego dostawcę
  - ***Prywatna*** – udostępniana przez wewnętrznego dostawcę
  - ***Community*** - udostępniana wspólnie przez wielu dostawców
  - ***Hybrydowa*** – kilka chmur o własnej tożsamości ale połączonych w jedną większą

AVET
Information and Network Security

Co dostajemy w ramach chmury

Typ infrastruktury

- **Infrastructure-as-a-Service** (IaaS) – dostarcza infrastrukturę IT
- **Software-as-a-Service** (SaaS) – dostarcza usługi za pomocą aplikacji
- **Platform-as-a-Service** (PaaS) – dostarcza gotowe platformy biznesowe
- **Communication-as-a-Service** (CaaS) – dostarcza usługi komunikacyjne

Najciekawsze rozwiązane dla Banków

- SaaS i PaaS
  - Zalety:
    - Obniżenie kosztów licencji
    - Obniżenie kosztów infrastruktury
    - Obniżenie kosztów wdrożenia
  - Wady:
    - SaaS: ograniczenie samej aplikacji / PaaS może być pozbawiony tej wady
  - Pytania:
    - Co tak naprawdę kupujemy
    - Ochrona danych
    - Ciągłość działania
    - Zgodność z przepisami
    - Stabilność dostawcy

AVET
Information and Network Security

5 MITÓW O CHMURZE

AVET
Information and Network Security

5 mitów

1. Chmura potrzebuje platformy wirtualizacyjnej. **Nieprawda:** wirtualizacja nie jest potrzebna do przetwarzania danych. Niektóre rozwiązania faktycznie wymagają takiej platformy wirtualizacyjnej. Najczęściej są to produkty firm, które mają takowe w swojej ofercie.
2. Chmura jest bezpieczniejsza od tradycyjnej sieci. **Nieprawda:** źle zabezpieczony system jest źle zabezpieczonym systemem niezależnie od modelu przetwarzania danych.
3. Chmura musi być dostarczana przez zewnętrznego dostawcę. **Nieprawda:** model prywatnej chmury pozwala na świadczenie usługi wewnętrznie.
4. Chmura nie może spełnić wymagań Nadzoru Bankowego. **Nieprawda:** wszystko zależy od zastosowanego modelu wdrożenia oraz sposobu używania chmury.
5. Chmura nie wymaga audytu bo jest bezpieczna. **Nieprawda:** każdy system wymaga kontroli niezależnie od dostawcy. Obowiązek ten jest nałożony także przez KNF i pojawia się między innymi w rekomendacji D

AVET
Information and Network Security

PODSTAWOWE ZAGROŻENIA

AVET
Information and Network Security

Podstawowe zagrożenia

Zagrożenia biznesowe

- Przywiązanie się do jednego dostawcy i jego bazy oprogramowania / narzędzi (tzw. cloud lock-in)
- Utrata kontroli nad swoimi danymi
- Nie spełnienie wymogów zgodności oraz prawnych

Zagrożenia wynikające ze zgodności

- Rekomendacja D i procedury inspekcji na miejscu GINB były pisane wiele lat przed obecnie dostępnymi rozwiązaniami
- Kwestie powierzenia przetwarzania danych stronie trzeciej i zabezpieczenie techniczne
- Ochrona prywatności i danych osobowych
  - Ustawa o ochronie danych osobowych
- Ochrona informacji finansowej
  - Prawo Bankowe
  - Ustawa o obrocie instrumentami finansowymi
- Wymogi związane z:
  - Zarządzaniem Ryzykiem Operacyjnym (BASEL II i Rekomendacja M)
  - PCI DSS
  - Wewnętrzne wymagania Banku i wdrożone standardy:
    - ISO 27001
    - ISO 20000
    - BS 25999

AVET
Information and Network Security

Skoro lista zagrożeń jest tak długa…

…DLACZEGO W TAKIM RAZIE MÓWIMY O CHMURZE?

AVET
Information and Network Security

Zalety chmury

- Błyskawiczna możliwość korzystania z usług:
  - Skrócenie czasu wytwarzania nowych aplikacji i infrastruktur
  - Niższe koszty projektu
  - Praktycznie brak czasu na integrację
  - Szybsze wdrażanie usług i produktów
  - Wielokrotnie mniejsze ryzyko projektowe
- Bezpieczeństwo:
  - Łatwiejsze zarządzanie bezpieczeństwem (jeden punkt wymagający ochrony zamiast wielu)
  - Niższe koszty utrzymania infrastruktury
  - Mniejsze zapotrzebowanie na zasoby ludzkie

AVET
Information and Network Security

Zalety z perspektywy Banków Spółdzielczych

- Niższe koszty
- Szybkie wdrażanie nowych usług (przy zachowaniu niskich kosztów)
- Mniejsze potrzeby zasobów ludzkich
- Konkurencyjność w starciu z bankami komercyjnymi

AVET
Information and Network Security

Modelowe rozwiązanie na przykładzie platformy **redcloudstorm**

CHMURA DLA BANKÓW SPÓŁDZIELCZYCH

AVET
Information and Network Security

Ważne pytania

- Czy rodzaj chmury ma znaczenie dla bezpieczeństwa?
- Czy technologia chmury ma znaczenie dla bezpieczeństwa?
- Czy technologia aplikacji ma znaczenie dla bezpieczeństwa?
- Czy aplikacje tradycyjne „wrzucone” do chmury stają się bardziej (nie)bezpieczne?
- Czy aplikacje tworzone z myślą o chmurze są bezpieczniejsze od tradycyjnych?
- Compliance…

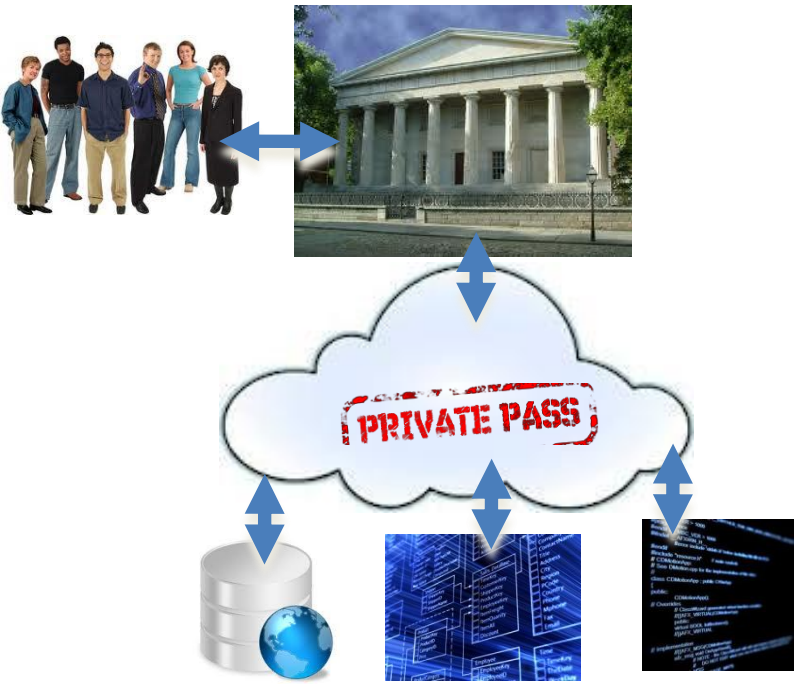
Czym jest redcloudstorm

- Niezależna platforma do budowania chmur, zwłaszcza typu PaaS: Private i Community
  - Pozwala budować chmury przy użyciu obecnej infrastruktury IT
  - Nie wymaga platformy wirtualizacyjnej = działa z każdą platformą wirtualizacyjną
  - Pozwala integrować fizyczne zasoby ze zwirtualizowanymi
  - Działa praktycznie na każdej platformie systemowej:
    - AIX, Linux, FreeBSD, OpenBSD, Windows 32/64
- Dostępna opcja microcloud

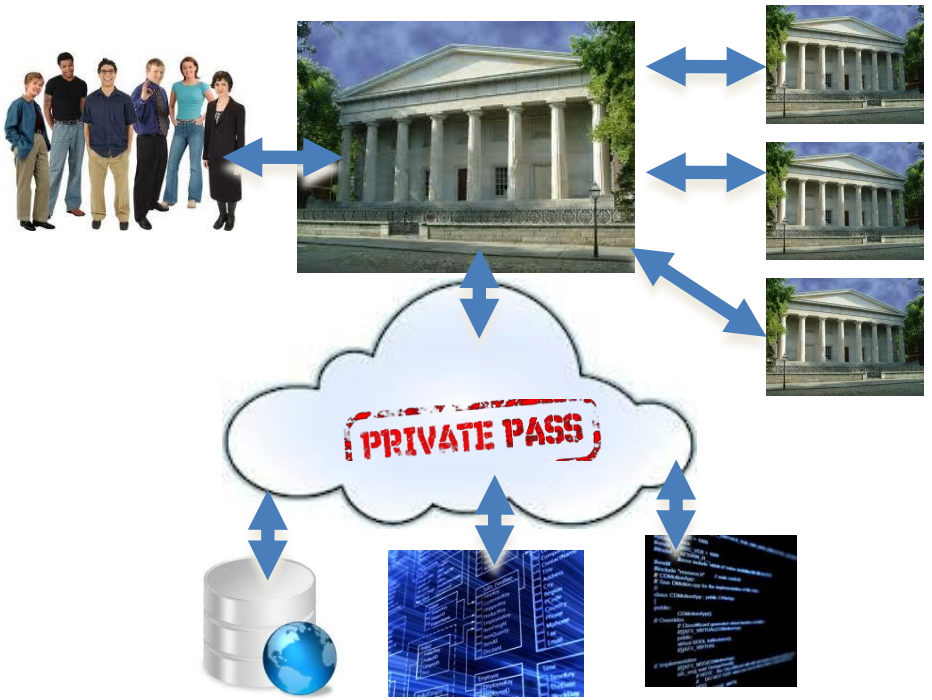
AVET
Information and Network Security

Docelowe rozwiązania (1/2)

Private PaaS



Private / Community PaaS



Docelowe rozwiązania (2/2)

Private PaaS microcloud

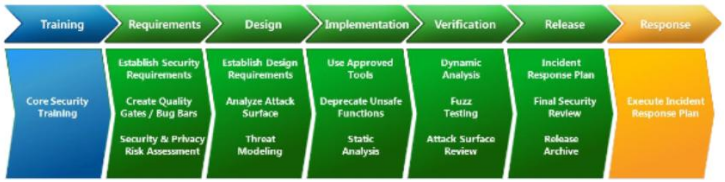
Model bezpieczeństwa

Wymogi

- Zgodność z przepisami sektora finansowego
- Niskie koszty
- Bezpieczna domyślna konfiguracja
- Integracja z obecnymi zabezpieczeniami
- Ochrona poufności i integralności
- Wysoka dostępność
  - Np. brak DNSu nie może zatrzymać przetwarzania
  - Replikacja danych
  - Brak jednego node'a chmury nie zaburza przetwarzania

Realizacja

- Wdrożenie Secure Development Lifecycle już w fazie projektowania rozwiązania



#20 Setup email address for security team postfix closed done

Setup email address for security team

AVET
Information and Network Security

Model bezpieczeństwa

Wymogi

- Zgodność z przepisami sektora finansowego
- Niskie koszty
- Bezpieczna domyślna konfiguracja
- Integracja z obecnymi zabezpieczeniami
- Ochrona poufności i integralności
- Wysoka dostępność
  - Np. brak DNSu nie może zatrzymać przetwarzania
  - Replikacja danych
  - Brak jednego node'a chmury nie zaburza przetwarzania

Realizacja

- Model Private PaaS
  - Zapewnienie zgodności
  - Wymuszenie odpowiednich zabezpieczeń
  - Uniemożliwienie błędnego / niebezpiecznego wdrożenia
- Wewnętrzna komunikacja
  - Użycie tunelu HTTPS
    - Ochrona poufności
    - Kontrola dostępu / uwierzytelnienie stron
    - Systemy zaporowe i IPS nie wymagają rekonfiguracji

AVET
Information and Network Security

Model bezpieczeństwa

Wymogi

- Zgodność z przepisami sektora finansowego
- Niskie koszty
- Bezpieczna domyślna konfiguracja
- Integracja z obecnymi zabezpieczeniami
- Ochrona poufności i integralności
- Wysoka dostępność
  - Np. brak DNSu nie może zatrzymać przetwarzania
  - Replikacja danych
  - Brak jednego node'a chmury nie zaburza przetwarzania

Realizacja

- Wbudowany DNS
- Praca bez DNS
- Nody chmury definiowane za pomocą IP
- Model pracy off-line (zwłaszcza przydatne w rozwiązaniu typu microcloud)

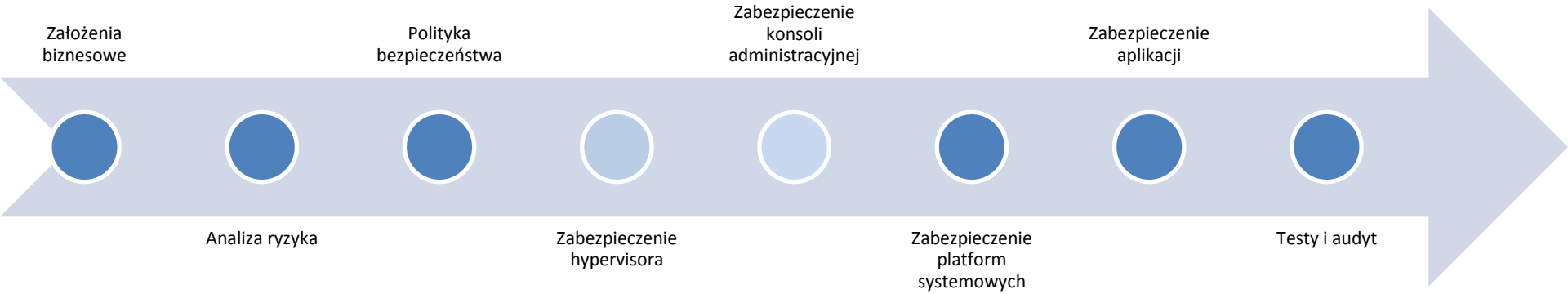
AVET
Information and Network Security

Krótki przewodnik

JAK STWORZYĆ BEZPIECZNĄ CHMURĘ?

AVET
Information and Network Security

Metodyka AVET INS



AVET
Information and Network Security

Przydatne publikacje

Dokumenty

- Guidance v2.1
- Cloud Controls Matrix v1.2
- VMware Infrastructure 3 Security Hardening
- vSphere 4.1 Hardening Guide
- Hardening Linuxa pod VMWare
- Proces SDL

AVET
Information and Network Security

Dziękuję za uwagę

- Pytania?

aleksander.czarnowski@avet.com.pl

AVET
Information and Network Security