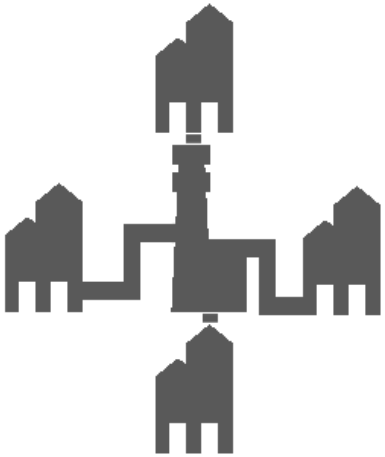
Wykorzystanie chmury w firmie produkcyjnej podzielonej na kilka oddziałów

Celem naszej pracy było ukazanie wykorzystania wydzierżawionej infrastruktury chmurowej w firmie produkującej rowery. Przypadek przedsiębiorstwa, które opisaliśmy, posiada kilka oddziałów zajmujących się produkcją części, które są składane w jedną całość w głównym oddziale, z którego wysyłane są zapotrzebowania na wyprodukowanie części do oddziałów podległych.

Piotr Krupa, Paweł Knapiński, Mateusz Kudelski

Przeznaczenie rozwiązania

- Płynność przepływu informacji między oddziałami w celu sprawniejszej realizacji
- posiadanie scentralizowanego i jednolitego oprogramowania



Cele i warunki do spełnienia

- zapewnienie stałego dopływu prądu
- zapewnienie stałego, redundantnego łącza internetowego
- zapewnienie szczelnego firewall'a
- tworzyć i przechowywać kopie zapasowe systemów
- zapewnienie fizycznej ochrony urządzeń i budynku przed utratą bądź przeciekiem danych
- zapewnienie stałego, szyfrowanego połączenia między oddziałami a serwerem (VPN S2S)
- łączenie do oddziału oddział do datacenter
- zapewnienie odpowiednio dużej przestrzeni dyskowej na dane firmy

Parametry techniczne rozwiązania

- Wydaje UPSy, oraz agregaty prądotwórcze
- stałe i szybkie przyłącza internetowe
- Wydajne i bezpieczne Firewall'y oraz antywirusy
- pojemne i szybkie dyski serwerowe
- wydajna pamięć RAM i procesor serwera

Zakres odpowiedzialności stron

1. Podpisanie umowy powierzenia i przetwarzania danych osobowych
Zleceniobiorca ponosi odpowiedzialność za dołożenie najwyższej staranności w wykonaniu wszelkich usług objętych przedmiotem Umowy.
2. Zleceniobiorca ponosi odpowiedzialność za poniesione szkody i utracone korzyści przez Zleceniodawcę do łącznej kwoty 100.000,00 (słownie: sto tysięcy) zł.
3. Zleceniobiorca nie ponosi odpowiedzialności za niewywiązanie się z warunków Umowy, jeżeli zostało to spowodowane przyczynami od niego niezależnymi (siła wyższa).
4. Zleceniobiorca odpowiada za działania wszystkich osób i innych podmiotów realizujących usługi w imieniu Zleceniobiorcy jak za własne działania, niezależnie od stosunku prawnego, który łączy go z taką osobą lub podmiotem.

Zakres odpowiedzialności stron

Zleceniobiorca nie ponosi odpowiedzialności za utratę danych przez Zleceniodawcę i niemożność
ich odtworzenia, jeżeli utrata ta i niemożność odtworzenia jest następstwem: nienależytego
serwisowania i utrzymania przez Zleceniodawcę sprzętu przechowującego kopię zapasową, awarii
sprzętu przechowującego kopię zapasową, utraty przez Zleceniodawcę kopii zapasowych,
okoliczności, nad którymi Zleceniobiorca nie ma rzeczywistej kontroli, są od niego niezależne, w
szczególności przypadkami siły wyższej lub innymi okolicznościami zaburzającymi pracę Beyond.pl,
niedostępności lub opóźnieniem w usługach świadczonych przez osoby trzecie na rzecz Klienta,
błędów oprogramowania dostarczanego przez osoby trzecie, ataków cybernetycznych (w tym
DDoS), usterki lub awarii sprzętu kontrolowanego przez Klienta, działania lub zaniechania Klienta
lub osób działających w jego imieniu, wykorzystania Usług w sposób sprzeczny z Umową.

Analiza bezpieczeństwa- audyt

Audyt bezpieczeństwa - cykliczne przeprowadzanie audytu bezpieczeństwa oddziałów poprzez weryfikację stanowisk pracowników (brak haseł na kartkach, pod klawiaturami, na monitorach), weryfikacja świadomości pracownika w zakresie niebezpiecznych wiadomości z nieznanymi załącznikami, linkami itp.. Kontrola programu antywirusowego na stacjach roboczych - ważność licencji oraz baz wirusów. Weryfikacja sieci lokalnej i urządzeń filtrujących ruch sieciowy - otwarte porty z zewnątrz, dostęp do sieci LAN poprzez gniazdka sieciowe (nie odłączone w krosownicy). Weryfikacja systemu wejścia/wyjścia oraz monitoringu. Utworzenie procedur regulujących dostęp do serwerowni, punktów dystrybucyjnych/krosowniczych.
Od strony samych systemów oraz maszyn fizycznych weryfikacja kopii urządzeń, analiza dostępności do danych z backupu,

Analiza bezpieczeństwa- monitorowanie

Monitorowanie bezpieczeństwa infrastruktury – Analiza logów systemowych z urządzeń sieciowych oraz maszyn serwerowych, posiadanie systemów monitorujących ruch sieciowy, pracę serwerów np. PRTG, skonfigurowane alerty w sytuacjach krytycznych (np. w momencie wykrycia kilku - kilkunastu nieudanych próbach logowania na urządzenie/a)

Utrzymanie- zapewnienie bezpieczeństwa technicznego i formalnego

-zastosowanie UPSów oraz listw antyprzepięciowych pozwoli przeciwdziałać spięciom, które mogłyby uszkodzić drogi sprzęt
-posiadanie zapasowych łączy internetowych pozwoli w razie awarii w dostawie internetu szybko przełączyć dostawcę i przywrócić stałą pracę w chmurze
-każdy pracownik posiadający dostęp do chmury podpisuje dodatkowo umowę powierzenia danych oraz klauzulę mówiącą o tym, że żadne dane nie wyjdą po za mury firmy

Utrzymanie- zapewnienie bezpieczeństwa technicznego i formalnego

-firewall'e oraz antywirusy, znajdujące się po stronie firmy wewnętrznej i zewnętrznej, muszą posiadać aktywną subskrypcję, dzięki czemu baza wirusów i nowych metod nieautoryzowanych wejść znajduje się w bazie programu antywirusowego co czyni korzystanie z zasobów chmurowych zdecydowanie bezpieczniejszym
-umowa zawarta pomiędzy firmą zewnętrzną a wewnętrzną zawiera również umowy powierzenia i przetwarzania danych osobowych, oraz precyzyjnie określa warunki świadczeń i płatności dla obu stron umowy
- w firmach wewnętrznych należy również zastosować najnowsze urządzenia sieciowe takie jak np. Routery czy switche, które dzięki swojej przepustowości i niezawodności powinny zapewnić stałą nieprzerwaną pracę w chmurze

Podsumowanie

- W części podsumowującej możemy potwierdzić, iż przedstawione przez nas rozwiązania informatyczne są skuteczne, stabilne a przede wszystkim bezpieczne. Każdy z nas posiada doświadczone w pewnych zakresach/kierunkach informatyki, które poruszyliśmy w tym dokumencie. Niemniej jednak rozwój informatyki jest tak dynamiczny, że sposobów na złamanie zabezpieczeń fizycznych, sprzętowych czy programowych pojawia się stosunkowo dużo. Zaproponowane przez nas rozwiązanie powinno skutecznie zabezpieczyć naszą firmę przed ewentualnymi atakami i szkodami.