

Outsourcing informatyczny i kolokacja - wady i zalety pod kątem wykorzystania w administracji

Jerzy Borys
p.o. naczelnika Wydziału Informatyki
Urząd Miasta Katowice
Jurek.Borys@um.katowice.pl

Outsourcing informatyczny i kolokacja – wady i zalety pod kątem wykorzystania w administracji

- Outsourcing, kolokacja i hosting
- Bezpieczeństwo, zagrożenia i sposoby gwarantowania określonego poziomu bezpieczeństwa
- Bezpieczeństwo przy zastosowaniu outsourcingu
- Outsourcing w Urzędzie Miasta Katowice
- Podsumowanie

Outsourcing, kolokacja i hosting

Outsourcing i netsourcing (def. Wikipedii):

Outsourcing (z ang. *out-source* - zewnętrzne źródło) to praktyka polegająca na **przeniesieniu części zadań wykonywanych przez firmę lub organizację z własnych pracowników na zewnętrznych kontrahentów.**

Najczęstszą przyczyną wprowadzania praktyk outsourcingowych jest chęć obniżenia kosztów i uniknięcia sytuacji korupcyjnych.

Netsourcing - odmiana outsourcingu, polegająca na **korzystaniu z aplikacji internetowych umieszczonych na zewnętrznym, wynajętym serwerze WWW, a nie na własnym, w ramach sieci firmowej.**

Forma ta jest w wielu sytuacjach możliwa dzięki faktowi, że przeglądarka internetowa jest uniwersalnym narzędziem dającym dostęp do wielu aplikacji.

Korzyścią z *netsourcingu* jest obniżanie kosztów dzięki specjalizacji firm - firma oferująca wielu przedsiębiorstwom usługi netsourcingowe może świadczyć je znacznie taniej niż w sytuacji, gdyby firmy te musiały instalować i obsługiwać własne serwery.

Outsourcing, kolokacja i hosting

Rodzaje outsourcingu:

Outsourcing pełny (strategic outsourcing) – przejście całej infrastruktury np. IT do firmy zewnętrznej.

W ramach tego typu kontraktu zawsze dochodzi do przejścia części pracowników instytucji zlecającej oraz odkupienia środków trwałych będących w jej posiadaniu.



Outsourcing selektywny - przekazanie firmie zewnętrznej kontroli nad wybranymi obszarami, (zarządzanie wybranymi aplikacjami, środowiskiem sieciowym, infrastrukturą internetową, itp.).

Outsourcing, kolokacja i hosting

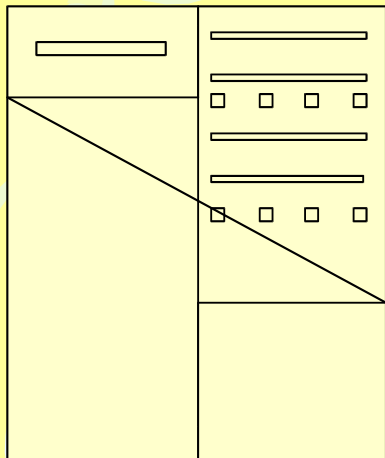
Przykłady outsourcingu:

- **Odtwarzanie środowiska IT po awarii** - identyfikacja obszarów krytycznych i analiza wpływu katastrofy na działalność jednostki, ocena i oszacowanie ryzyka w oparciu o analizę głównych procesów biznesowych, opracowanie planów zapewniających ciągłość procesów biznesowych (w tym planu likwidacji skutków potencjalnej awarii) oraz wdrożenie, przeprowadzeniu testów i stała aktualizacja tych planów.
- **Zarządzanie infrastrukturą informatyczną** - kompleksowa usługa zarządzania środowiskiem komputerów osobistych Klienta - stacjonarnymi komputerami PC, komputerami przenośnymi, drukarkami, serwerami plików, serwerami wydruku oraz HelpDesk na wszystkich etapach jego życia, poczynając od procesu zakupu infrastruktury (procurement), poprzez instalację nowego sprzętu, dystrybucją oprogramowania, przeprowadzanie procesu wszelkich zmian i uaktualnień, serwisowanie całej platformy, aż po utylizację zużytego sprzętu
- **Zarządzanie infrastrukturą internetową** - udostępnienie internetowego centrum danych - platformy sprzętowej i odpowiedniego oprogramowania, a także usług związanych z tworzeniem i zarządzaniem specjalistycznymi portalami lub serwisami internetowymi.
- **Infrastruktura na żądanie (On Demand)** - instalowanie w siedzibie Klienta lub w centrum danych nadmiarowej infrastruktury - kiedy działająca platforma przestaje być wystarczająca i niezbędne staje się uruchomienie dodatkowej infrastruktury, wówczas w bardzo krótkim czasie uruchamiane są kolejne, zainstalowane już jednostki. Istnieje kilka wariantów tej usługi, przy czym dwa są najbardziej popularne:
 - korzystanie z dodatkowych zasobów tylko w okresach wzmożonej aktywności przedsiębiorstwa,
 - stałe powiększanie wykorzystywanych zasobów w miarę rozwoju firmy.W obydwu przypadkach Klient płaci za faktycznie użytkowaną infrastrukturę.
- **Zarządzanie Aplikacjami** - utrzymywanie wysokiej dostępności krytycznych dla przedsiębiorstwa aplikacji, takich jak np. systemy ERP. polegające na stworzenie odpowiedniej architektury systemu, proaktywne działania zapobiegające awariom, instalację wysoce zaawansowanych systemów monitorujących środowisko, zarządzanie siecią, a także wykorzystywanie zaawansowanych systemów do zautomatyzowanego wykonywania kopii zapasowych.

Outsourcing, kolokacja i hosting

Hosting i kolokacja (def. Wikipedii):

Hosting - usługa świadczona przez ISP polegająca na **udostępnieniu zasobów serwerowni oraz wynajmie platformy sprzętowej lub wirtualnej platformy systemowej**. W ramach usługi klient może otrzymywać dostęp do środowiska systemu operacyjnego o określonych umową parametrach, dostęp do sieci, zasilanie i wsparcie administratorów. Typowa usługa zwłaszcza w zakresie wynajmu platform pod serwery HTTP - web hosting



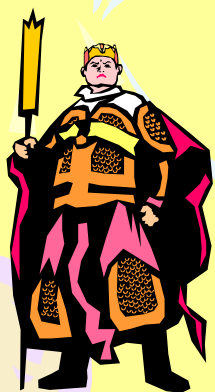
Kolokacja informat. usługa świadczona przez ISP polegająca na **udostępnieniu zasobów serwerowni**. W ramach usługi klient może otrzymywać miejsce w szafie serwerowej, dostęp do sieci, zasilanie i wsparcie administratorów, samemu dostarczając serwer(y) czym różni się ta usługa od hostingu.



Outsourcing, kolokacja i hosting

Przykłady usług w ramach hostingu:

- Wynajmowanie klientowi przestrzeni dyskowej o określonym rozmiarze
- Utrzymanie domeny klienta na serwerach DNS usługodawcy
- Utrzymanie skrzynek pocztowych i aliasów do skrzynek pocztowych we własnej domenie klienta
- Webmail (odbiór poczty przez WWW)
- Utrzymanie stron WWW
- Graficzne statystyki stron WWW
- Dostęp przez FTP
- Obsługa skryptów CGI
- Blokada dostępu do strony WWW/Katalogu (.htaccess)
- Udostępnianie baz danych MySQL, PostgreSQL
- Wykonywanie kopii bezpieczeństwa
- Utrzymanie Biuletynu Informacji Publicznej



Outsourcing, kolokacja i hosting

Przykłady usług w ramach kolokacji:

- dzierżawa miejsca w serwerowni na serwery i inne urządzenia sieciowe
- nieobciążone łącze do Internetu
- obsługa domen
- utrzymanie podstawowego i zapasowego serwera DNS
- zapewnienie awaryjnego zasilania, klimatyzowanego pomieszczenia i całodobowej ochrony
- "reset" i dostęp fizyczny do urządzeń
- pomoc w przypadku awarii sprzętu
- możliwość przeprowadzenia testów
- opieka administratora nad serwerem internetowym
- zapewnienie bezpieczeństwa fizycznego serwera i zabezpieczenie danych

Bezpieczeństwo, zagrożenia i sposoby gwarantowania określonego poziomu bezpieczeństwa

Bezpieczeństwo teleinformatyczne (def. Wikipedii):

Bezpieczeństwo teleinformatyczne to inaczej bezpieczeństwo informacji i systemów teleinformatycznych rozpatrywane w odniesieniu do instytucji wykorzystującej lub udostępniającej infrastrukturę teleinformatyczną aby osiągnąć wyznaczone cele. (...)
Bezpieczeństwo w ujęciu całościowym powinno obejmować aspekt organizacyjny, techniczny i prawny.

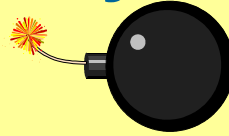
Bezpieczeństwo rozpatrywać można na trzech poziomach:

- instytucji - na tym poziomie chroniona jest: ciągłość misji, ciągłość procesów biznesowych, zdolność świadczenia usług, reputacja, działanie zgodne z prawem**
- infrastruktury teleinformatycznej - ochronie na tym poziomie podlegają: zasoby informacji, oprogramowanie, sprzęt, kadry, dokumenty (w tym dotyczące eksploatacji oraz samych zabezpieczeń)**
- poszczególnych systemów - operuje się tu terminem polityki bezpieczeństwa systemu teleinformatycznego, która przedstawiona jest jako zestaw praw, reguł i praktycznych doświadczeń ustalających sposób zarządzania, ochrony i dystrybucji informacji wrażliwej wewnątrz określonego systemu.**

Bezpieczeństwo, zagrożenia i sposoby gwarantowania określonego poziomu bezpieczeństwa

Systemy teleinformatyczne – główne zagrożenia:

Główne zagrożenia:



- zewnętrzne:

- włamania i kradzież urządzeń komputerowych

- wirusy i robaki internetowe

- ataki typu DoS

- działania hackerów zmierzające do podmiany informacji przechowywanych w systemach

- działania hackerów zmierzające do przejęcia kontroli nad systemami

- wewnętrzne:

- błąd użytkownika

- zanik zasilania

- awaria sprzętu

- błędy w oprogramowaniu systemowym, bazodanowym i aplikacyjnym

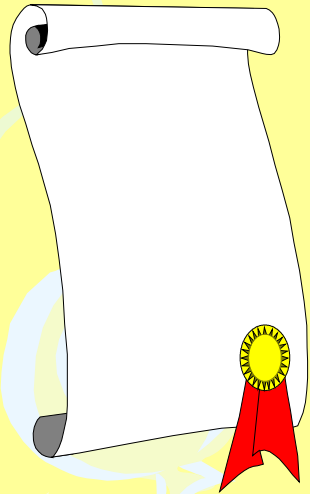
- błąd administratora systemu



Bezpieczeństwo przy zastosowaniu outsourcingu

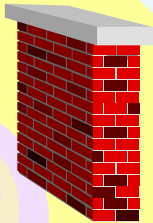
Bezpieczeństwo outsourcingu pełnego:

+ Przerzucenie odpowiedzialności za bezpieczeństwo powierzonych zasobów na usługodawcę:



- kontrolę fizycznego dostępu do systemu zabezpiecza usługodawca
- kopie bezpieczeństwa wykonuje usługodawca
- zasilanie awaryjne zabezpiecza usługodawca
- usługodawca dba o instalowanie łat do oprogramowania
- usługodawca zapewnia oprogramowanie antywirusowe
- usługodawca odpowiada za takie zdublowanie zasobów sprzętowych, aby przestoje mieściły się w zadanym w umowie czasie

+ Fizyczne odseparowanie powierzonych zasobów od zasobów wewnętrznych instytucji



- mniejsze prawdopodobieństwo zainfekowania sieci wewnętrznej wirusami lub robakami internetowymi
- mniejsze prawdopodobieństwo uzyskanie kontroli nad siecią wewnętrzną

ALE

- Większa wrażliwość (w powierzonych zasobach) na ataki typu DoS
- Brak kontroli nad strategicznymi zasobami instytucji

Bezpieczeństwo przy zastosowaniu outsourcingu

Bezpieczeństwo hostingu:

+ Przerzucenie odpowiedzialności za bezpieczeństwo powierzonych danych na usługodawcę:



- kontrolę fizycznego dostępu do systemu zabezpiecza usługodawca
- kopie bezpieczeństwa wykonuje usługodawca
- zasilanie awaryjne zabezpiecza usługodawca
- usługodawca zapewnia oprogramowanie antywirusowe
- usługodawca dba o instalowanie łat do oprogramowania
- usługodawca odpowiada za takie zdublowanie zasobów sprzętowych, aby przestoje mieściły się w zadanym w umowie czasie

ALE

- Fizyczne odseparowanie powierzonych danych od zasobów wewnętrznych instytucji



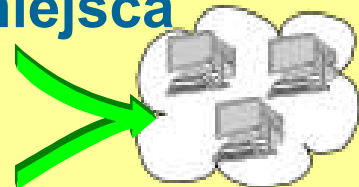
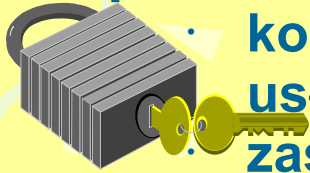
- większe prawdopodobieństwo przejęcia danych służących do uwierzytelniania użytkownika w bazie danych
- większe prawdopodobieństwo zablokowania dostępu do danych przy użyciu ataków typu DoS

- Mniejszy wybór rodzajów baz danych

Bezpieczeństwo przy zastosowaniu outsourcingu

Bezpieczeństwo kolokacji (plusy):

- + Przerzucenie odpowiedzialności za bezpieczeństwo powierzonych sprzętu i jego dostępności na usługodawcę:
 - kontrolę fizycznego dostępu do systemu zabezpiecza usługodawca
 - zasilanie awaryjne zabezpiecza usługodawca
 - usługodawca odpowiada za takie zdublowanie łączy i urządzeń sieciowych, aby przestoje mieściły się w zadanym w umowie czasie
- + Fizyczne odseparowanie powierzonych zasobów od zasobów wewnętrznych instytucji
 - mniejsze prawdopodobieństwo zainfekowania sieci wewnętrznej wirusami lub robakami internetowymi
 - mniejsze prawdopodobieństwo uzyskanie kontroli nad siecią wewnętrzną
- + Umożliwienie dostępu do systemu niezależnie od miejsca pobytu użytkownika



Bezpieczeństwo przy zastosowaniu outsourcingu

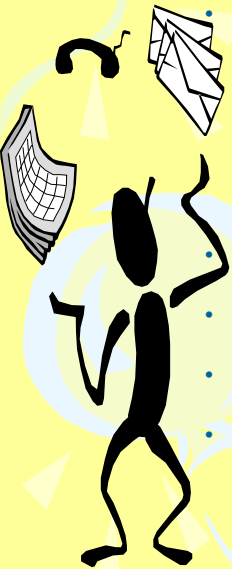
Bezpieczeństwo kolokacji (minusy):

- Odpowiedzialność za bezpieczeństwo systemu ponosi zlecający:

zlecający odpowiada za dostęp logiczny – musi zapewnić odpowiednio skonfigurowany router ze ścianą ogniową tak, aby dostęp do zasobów był zgodny z polityką bezpieczeństwa

- zlecający musi dbać o kopie bezpieczeństwa
- zlecający musi dbać o instalowanie łat do oprogramowania
- zlecający musi dbać o oprogramowanie antywirusowe
- zlecający musi zabezpieczyć takie zdublowanie zasobów sprzętowych i zapewnić serwis, aby przestoje mieściły się w zadanym w polityce bezpieczeństwa czasie

- Większe prawdopodobieństwo przejęcia danych służących do uwierzytelniania użytkownika w systemie
- Większe prawdopodobieństwo zablokowania dostępu do danych przy użyciu ataków typu DoS



Outsourcing w Urzędzie Miasta Katowice

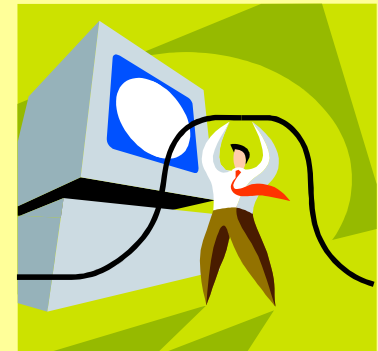
Outsourcing pełny:

- System praw jazdy
- System rejestracji pojazdów
- System dowodów osobistych



Outsourcing częściowy:

- Serwis sprzętu komputerowego
- Serwis oprogramowania systemowego i bazodanowego





Outsourcing w Urzędzie Miasta Katowice

Hosting:

- Serwis WWW Urzędu Miasta Katowice
- Biuletyn Informacji Publicznej Urzędu Miasta Katowice
- Biuletyn Informacji Publicznej jednostek miejskich podległych Urzędowi Miasta Katowic
- System publikowania ogłoszeń o zamówienia publiczne Urzędu Miasta Katowice
- System publikowania ogłoszeń o zamówienia publiczne jednostek miejskich podległych Urzędowi Miasta Katowic

URZĄD MIASTA
KATOWICE

40-098 Katowice, ul. Młyńska 4, tel. 2593-90



BIULETYN INFORMACJI PUBLICZNEJ
Urzędu Miasta Katowice <http://bip.um.katowice.pl>

Kolokacja:

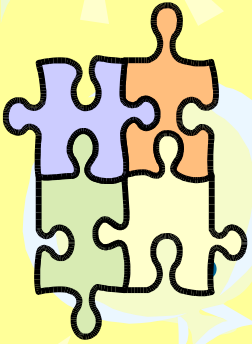
- Kolokacja serwera ArcIMS wraz z routerem zabezpieczającym



Podsumowanie

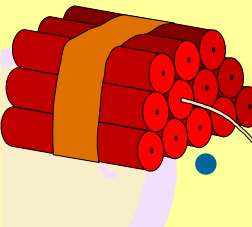


- Decyzja o powierzeniu określonych zadań do realizacji na zewnątrz i wyborze rodzaju outsourcingu powinna być poprzedzona analizą biznesową z uwzględnieniem założeń polityki bezpieczeństwa instytucji.



- Im pełniejszy zakres outsourcingu, tym wyższy poziom bezpieczeństwa systemów i danych (pod warunkiem wyboru partnera gwarantującego określony poziom usług), ale większe uzależnienie od usługodawcy

Outsourcing częściowy (netsourcing, hosting, kolokacja) nie „załatwia” wszystkich problemów związanych z bezpieczeństwem – zawsze należy działać zgodnie z aktualizowaną na bieżąco polityką bezpieczeństwa.



BEZPIECZEŃSTWA NIE MOŻNA KUPIĆ !

NIE ISTNIEJE BEZPIECZEŃSTWO STUPROCENTOWE !

Dziękuję za uwagę



Pytania ?

Jerzy Borys
Jurek.Borys@um.katowice.pl