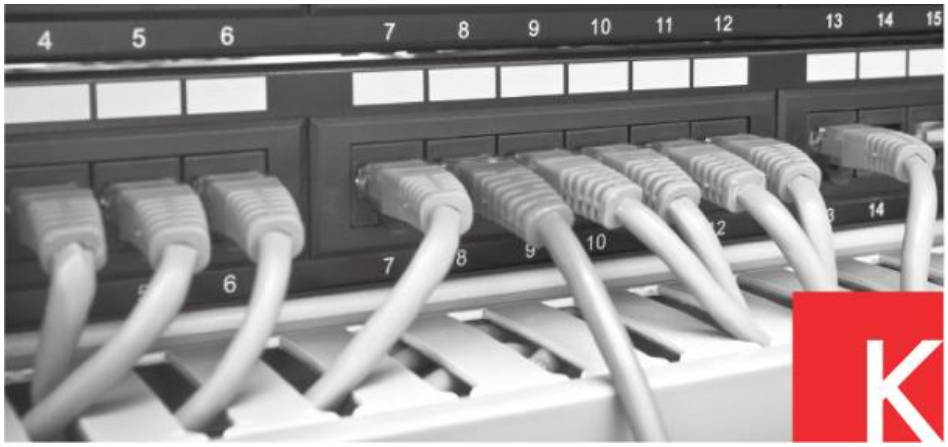
2012

Przewodnik cloud computing

veracity

Niniejszy przewodnik jest przeznaczony dla osób, które chcą dowiedzieć się na czym polegają usługi cloud computing oraz w jaki sposób ocenić te usługi pod kątem bezpieczeństwa.



Fundacja Veracity
2012-08-07

Spis treści

Veracity

Wprowadzenie

Rozwój przemysłu komputerowego powoli zatacza koło.

Początki komputeryzacji to lata 40-ste XX wieku, kiedy to powstały pierwsze komputery jak ENIAC, Colossus, Z3 czy też ABC. Mało kto przypuszczał wtedy jak komputery zmienią świat:

Oceniam potrzeby światowego rynku na około pięć komputerów.

Thomas Watson, prezes IBM, 1943r

Komputery w tym czasie składały się z mocnej jednostki serwerowej służącej do przetwarzania danych oraz z terminali, które umożliwiały zlecanie wykonania poszczególnych działań i tym samym nie musiały cechować się dużą wydajnością.

Lata 70-te to początki komputerów osobistych i tym razem wiele osób nie wierzyło, iż komputery zagoszczą w naszych domach:

"Nie ma powodu, aby indywidualna osoba miała komputer w domu."

Ken Olson, prezes i założyciel Digital Equipment Corp. 1977 r

Stało się jednak inaczej. Rola komputerów osobistych znacząco rosła. Tworzone nowe systemy operacyjne oraz oprogramowanie wpłynęły na dynamiczny rozwój wydajności komputerów osobistych. Różnice pomiędzy powszechnie stosowanymi serwerami a stacjami roboczymi zaczęły się zacierać. Niska przepustowość łącz sieciowych powodowała, iż każdy komputer przetwarzał lokalnie większość danych.

Ostatnie lata przynoszą popularyzację coraz to szybszego Internetu, co przyczynia się do powrotu idei ośrodków przetwarzania dane, które realizują usługi dla stacji roboczych mających charakter terminali.

Dochodzimy tutaj do tematu chmur obliczeniowych czyli cloud computingu zwanego w Polsce popularnie chmurą.

Rodzaje cloud computing

- Private Cloud –w tym przypadku infrastruktura i zasoby IT należą do Klienta. Rozwiązanie takie zapewnia elastyczniejsze i efektywniejsze zarządzanie własnym środowiskiem informatycznym.
- Hybrid Cloud – jest rozwiązaniem, które umożliwia Klientom skorzystanie z zewnętrznych zasobów IT w celu pokrycia nadwyżek zapotrzebowania na moc. Dzięki rozwiązaniu Hybrid Cloud można wykupić moc obliczeniową na zdalnych serwerach tylko wtedy, kiedy jest rzeczywiście potrzebna i w wymaganych ilościach.
- Public Cloud – w tym przypadku Klient korzysta z zasobów IT dostępnych na zewnątrz (zdalnie), jednocześnie określając swoje wymagania odnośnie mocy obliczeniowej/pamięci oraz funkcjonalności i dostępności usług.

Modele cloud computing

- Kolokacja – model ten polega na wynajęciu pomieszczenia serwerowni, dostępu do energii elektrycznej, klimatyzacji i dostępu do Internetu. Klient we własnym zakresie organizuje pozostałe elementy jak sprzęt, systemy operacyjne, zabezpieczenia, oprogramowanie i aplikacje.
- IaaS – Infrastructure as a Service (Infrastruktura jako usługa) – w tym modelu Klient otrzymuje od dostawcy infrastrukturę informatyczną (sprzęt, oprogramowanie oraz serwisowanie). Klient często dostarcza dostawcy własne oprogramowanie do zainstalowania na wynajmowanym sprzęcie.
- PaaS – Platform as a Service (Platforma jako usługa) – dostawca zapewnia Klientowi dostęp do gotowych aplikacji poprzez interfejs. W tym przypadku najczęściej Klient nie musi instalować na komputerze dodatkowego oprogramowania, tym samym więc ma dostęp do aplikacji z dowolnego połączonego z Internetem komputera.
- SaaS – Software as a Service (Oprogramowanie jako usługa) – klient otrzymuje konkretne funkcjonalności i oprogramowanie. Zapłata następuje za każdorazowe użycie oprogramowania, a dostęp uzyskiwany jest na żądanie.
- CaaS – Communications as a Service (Komunikacja jako usługa) – usługodawca zapewnia platformę pod telekomunikacyjne środowisko pracy.
- DaaS – Desktop as a Service (Stacja robocza jako usługa) - w tym modelu użytkownik otrzymuje kompletną maszynę wirtualną, w pełni spersonalizowaną, a stacja robocza z której korzysta stanowi tzw. cienkiego Klientem i nie posiada danych ani funkcjonalnego oprogramowania.

Korzyści cloud computing

Cloud computing jest rozwiązaniem, które może być wykorzystywane zarówno przez małe, średnie jak i duże organizacje. Właściwie zaprojektowane rozwiązanie spełniające potrzeby Klienta może przynosić wiele korzyści:

- rozwiązanie dostosowane do aktualnych potrzeb (w tradycyjnym IT realizowane inwestycje uwzględniają często duży bufor, zakładając rozwój firmy/usług, wzrost zapotrzebowania na moc wraz z rozwojem oprogramowania itp., przez co poziom wykorzystania zasobów w tradycyjnym IT wynosi mniej niż 30%);
- znaczne skrócenie czasu wdrożenia nowego rozwiązania informatycznego/usługi, jak również skrócenie czasu zarządzania zmianą, jak i zwalniania zasobów i usług;
- niższe koszty początkowe oraz znacznie krótszy zwrot z inwestycji wdrożenia nowego rozwiązania/usługi IT;
- elastyczność / skalowalność rozwiązań;
- mobilność.

Bezpieczeństwo cloud computingu – audyt dostawcy

Teoretycznie chmura powinna zapewniać większe bezpieczeństwo danych niż środowisko IT utrzymywane własnym kosztem. Cloud computing oferują zazwyczaj duże firmy o sporym kapitale które stać na drogie i efektywne zabezpieczenia. Serwerownie przypominają często bunkry odporne na wszelkiego rodzaju zagrożenia fizyczne począwszy od zalania/powodzi a skończywszy na bombardowaniu budynku. Bezpieczeństwa logicznego pilnują potrzebne firewall'e, systemy antywirusowe, IDS, IPS i wiele innych rozwiązań podnoszących bezpieczeństwo. I zazwyczaj w rzeczywistości tak jest, ale zdarzają się również głośne przypadki jak choćby awaria serwerów jednego z największych graczy na rynku – Beyond.pl, firmy kładącej duży nacisk na bezpieczeństwo. Podczas przerwy w dostawie usług spowodowanej trzyminutową awarią prądu kilka dużych polskich portali internetowych przestała działać, a użytkownicy prywatni, którzy utrzymywali swoje dane na serwerach Beyond.pl utracili je bezpowrotnie.

Prawdziwą plagą jest dostępność usług. Chmura z założenia ma oferować usługi dla wielu organizacji - najlepiej od kilkudziesięciu do kilkuset. W przypadku „zablokowania" dostępu do usług nagle kilkaset firm nie ma dostępu do danych. Zaczynają urywać się telefony na pierwszej linii wsparcia i klienci stają się nerwowi. W przypadku niektórych usług klienci w każdej godzinie braku dostępu do usługi tracą setki tysięcy złotych. Organizacje przestępcze lub jak kto woli hakerskie terroryzują centra przetwarzania danych atakami DOS (Denial of Services). Polega to na zasypaniu serwerów milionami zapytań płynących z sieci. Serwery nie nadążają z przetwarzaniem takiej ilości danych i usługi przestają być dostępne. Przed tego typu atakiem bardzo trudno się obronić, dlatego jest on obecnie największym ryzykiem cloud computingu.

Naruszenie zabezpieczeń w środowisku przetwarzania w chmurze może niekorzystnie wpłynąć na newralgiczne obszary działalności organizacji i stworzyć zagrożenie dla użytkowników usług oraz danych. Punktem wyjścia do bezpiecznego przetwarzania w chmurze jest ocena i analiza skuteczności istniejących zabezpieczeń, rozpoznanie luk w systemie zabezpieczeń i podjęcie działań naprawczych zmierzających do podniesienia ogólnego poziomu bezpieczeństwa chmury.

Analiza bezpieczeństwa środowisk cloud computing obejmować powinna m.in. następujące obszary:

- bezpieczeństwo fizyczne;
- bezpieczeństwo aplikacji / analiza kodu źródłowego;
- zabezpieczenie sieci teleinformatycznej;
- zarządzanie tożsamością i dostępem do aplikacji;
- zarządzanie kopiami zapasowymi;
- zarządzanie zmianami/aktualizacjami w systemach teleinformatycznych.

Do oceny środowiska cloud computing można wykorzystać standard opracowany w tym celu: Security Guidance for Critical Areas of Focus in Cloud Computing.

Do oceny stosowanych praktyk zastosować można również inne międzynarodowe standardy jak: ISO 27001, ISO 27002, ISO 20000, ITIL itp.

Klient korzystający z usług dużego, często międzynarodowego dostawcy usług cloud computing, nie ma często możliwości analizy bezpieczeństwa proponowanych usług. W tym przypadku zaufać musi renomie dostawcy i ew. przeanalizować dane dotyczące bezpieczeństwa podane przez dostawcę usług.

Uwagę zwrócić należy w tym przypadku m.in. na zabezpieczenie/szyfrowanie połączenia, częstotliwość i zakres wykonywanych kopii zapasowych, stosowane metody uwierzytelnienia (hasła/tokeny), jak również zapewnienie supportu IT ze strony dostawcy, który umożliwi ew. szybkie rozwiązanie problemów.

Oprócz bezpieczeństwa danych ważne dla większości użytkowników powinny być zastosowane mechanizmy uwolnienia danych z chmury. W szczególności w architekturze SaaS

Cloud computing a ochrona danych osobowych

Danymi osobowymi są wszelkie informacje dotyczące konkretnej osoby, za pomocą których bez większego wysiłku i kosztu można tę osobę zidentyfikować. Przykładowe dane osobowe to imię, nazwisko oraz adres zamieszkania lub np. PESEL. Przykładowe zbiory danych osobowych: dane osobowe pracowników zatrudnionych w organizacji (teczki pracowników, system kadrowo-płacowy, dokumenty MS Excel), dane osobowe kandydatów do pracy (listy motywacyjne, CV w wersji papierowej oraz elektronicznej), dane

osobowe kierowców (dedykowany system informatyczny, dokumentacja papierowa), dane osobowe klientów (dedykowany system informatyczny, dokumentacja papierowa), dane osobowe kontrahentów – osoby prowadzące działalność gospodarczą (dedykowany system informatyczny, dokumentacja papierowa), itp.

Mówiąc o przetwarzaniu danych osobowych, należy uwzględnić wszelkie operacje, jakie można wykonać na danych w tym m.in. ich przechowywanie, udostępnianie, zmienianie, modyfikowanie, przekazywanie, zbieranie, utrwalanie i opracowywanie.

Tym samym każda firma, która ma zatrudnionego minimum jednego pracownika i/lub posiada dane swoich klientów, którymi są osoby fizyczne, przetwarza dane osobowe i będąc administratorem tych danych zobowiązana jest prawnie przestrzegać wymagań zdefiniowanych w ustawie o ochronie danych osobowych oraz w dedykowanym rozporządzeniu MSWiA.

W przypadku, gdy dane te chcemy przetwarzać lub chociażby przechowywać u dostawcy cloud computing, powinniśmy zarówno my jak i usługodawca spełnić wymagania zawarte w ustawie i rozporządzaniu o ochronie danych osobowych. Podstawowym elementem w tym zakresie jest formalna podstawa współpracy i powierzenia danych - czyli spisana umowa o powierzeniu przetwarzania danych osobowych. Szczególną uwagę należy zwrócić na dodatkowe wymagania występujące w przypadku, gdy nasze dane przetwarzane są poza Polską a tym bardziej poza Unią Europejską.

Podsumowanie

Przyszłość Chmury nie jest taka jasna jak się wszystkim wydaje. Po kilku latach funkcjonowania nowej/starej filozofii uczucia są mieszane. Wiele małych i średnich firm chwali sobie cloud computing za obniżenie kosztów oraz dużą elastyczność. Duże firmy często pozostaja przy swoich serwerach, a są też takie przypadki jak General Motors które korzystały z chmury a obecnie się z niej wycofują. Szybki rozwój rynku usług Cloud computingu powoduje powstawanie coraz to nowych firm proponujących swoje usługi w tym zakresie. Część z tych firm nie jest jednak wystarczająco przygotowana do realizacji usług na wysokim poziomie pod względem jakości oraz niezawodności. Oddając nasze dane w cudze ręce musimy wziąć to ryzyko pod uwagę i ew. zminimalizować je poprzez analizę bezpieczeństwa usług dostawcy czy to przeprowadzoną w ramach audytu czy też w ramach analizy szczegółowych danych technicznych. Wiarygodności dostawcy usług dodają również pozytywne oceny Klientów, jak również certyfikaty potwierdzające stosowanie dobrych praktyk w zakresie IT oraz bezpieczeństwa, wystawiane przez niezależne organizacje.

Veracity