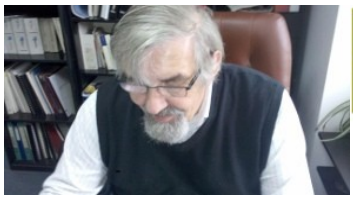


Old Man GURU Magazine

Wychodzi bardzo nieregularnie, kiedy wydaje mi się, że mam coś ciekawego lub pożytecznego do napisania...

Numer 23/2011 5 grudzień 2011

No i na co mi przyszło na stare lata – zdawać egzaminy! Na całe szczęście udało mi się uniknąć kompromitacji i uzyskałem certyfikaty RHCSA (RedHat Certified System Administrator) oraz RHCE (RedHat Certified Engineer) za pierwszym podejściem. Muszę podkreślić znakomitą atmosferę panującą w firmie Compendium, dzięki której udało mi się uniknąć silnego stresu związanego ze zdawaniem egzaminu przez osobę z grupy wiekowej 60+.

Wyjaśnia to także przerwę w pisaniu „Old Man GURU" ponieważ musiałem się po prostu „nieco" douczyć – coś jednak od czasów, gdy uzyskiwałem tytuł „SCO Authorised Engineer" i „SCO Authorised Instructor" w systemach operacyjnych się zmieniło. Sam egzamin jednak bardzo mi się podobał – przede wszystkim dlatego, że polega wyłącznie na realizowaniu praktycznych zadań na „żywym" systemie. Unika się więc zgadywania „oczekiwanych odpowiedzi" na pytania testowe – liczy się jedynie efekt. Problemem (przynajmniej dla mnie) był czas – zmieściłem się w nim "na styk", ale to może problem wynikający z mojego wieku – w końcu jestem już od niedawna prawdziwym dziadkiem.

Pora jednak przejść „do rzeczy". Stosunkowo niedawno wygłaszałem referat na Konferencji CPI w Jachrance, lecz miałem również okazję wysłuchać bardzo ciekawej prezentacji Artura Cyganka z CITRIX'a (swoją drogą „stara wiara z SCO" się dobrze trzyma). Jedną z jej głównych tez było zasygnalizowanie coraz powszechniejszego zjawiska polegającego na wykorzystywaniu tego samego sprzętu komputerowego do pracy zawodowej oraz do celów prywatnych. Artur przywołał szereg przykładów z USA, ale przecież każdy z nas obserwuje je wokół siebie. Popularność komputerów przenośnych spowodowała, że na biurkach w firmach coraz częściej widzimy notebooki i netbooki, w ekspresach coraz powszechniejsze w użyciu są tablety, a na ulicach spotykamy sporo ludzi dźwigających charakterystyczne torby... Mój stosunkowo niedawno kupiony notebook posiada oczywiście wyjście HDMI, którego cel wydaje się być dość oczywisty – podłączenie do telewizora LCD (oczywiście w standardzie HD). A więc wielu z nas komputer przenośny (niezależnie od typu) zaczyna towarzyszyć przez cały dzień i jego oprogramowanie musi być więc uniwersalne tak, aby można go było używać zarówno w pracy do realizacje zadań służbowych jak i w domu do odtwarzania filmów oraz do gier. Obsługa Internetu jest oczywista – korzystamy z sieci zarówno w pracy, jak i w domu, pociągu, hotelu itp.

System operacyjny komputera osobistego (zwłaszcza przenośnego) musi więc być uniwersalny. Wystarczy rozejrzeć się wokół, aby stwierdzić, że na komputerach osobistych praktycznie niepodzielnie króluje system MS Windows. Nie ma w tym nic dziwnego – wszak od swych narodzin był on projektowany pod kątem potrzeb użytkowników komputerów osobistych. Wielu entuzjastów Linuksa marzy o zdetronizowaniu Windowsów,

jednak pozycja MS Windows na tym rynku nie ulega znaczącej zmianie. Proszę pamiętać, że pisze to osoba, która na swym notebooku używa na co dzień (zarówno w pracy, jak i w domu) Linuksa (SuSE Linux Enterprise Desktop). Wynika to jednak przede wszystkim z moich osobistych przyzwyczajeń – bo prawie zawsze korzystałem z systemów określanych jako „UNIX-like" - od XENIX'a począwszy, zaś ze środowiska X Window od wersji X11R3. I choć wielu moich studentów oraz znajomych stwierdza ze zdziwieniem patrząc na ekran mojego komputera „to to jest ten LINUX?" nie mam zamiaru nikogo na siłę „ewangalizować".

Oczywiście można podać szereg przykładów, które udowodniają, że możliwe jest wykorzystywane Linuksa na komputerach osobistych. Warto jednak zwrócić uwagę, że najczęściej Linux jest wówczas wykorzystywany w ściśle określonym celu. Są to na przykład terminale sieciowe, końcówki informacyjne, kioski internetowe, systemy biblioteczne a nawet stanowiska w pracowniach szkolnych. Zastosowania te łączy jedna wspólna cecha – system jest konfigurowany przez specjalistę – niezależnie od tego, czy jest to profesjonalista czy też entuzjasta wolontariusz lub po prostu kolega (ew. koleżanka). Użytkownicy po prostu korzystają z przygotowanego przez nich stanowiska i najczęściej nie dokonują żadnych modyfikacji systemu. W takich przypadkach Linux sprawdza się znakomicie oczywiście po warunkiem, że został poprawnie zainstalowany oraz skonfigurowany. Różnice w obsłudze pulpitu Linuksa (gnome, kde czy xfce) a pulpitu MS Windows są bardzo niewielkie i użytkownicy radzą sobie w obu środowiskach znakomicie, a nawet w większości przypadków nie zauważają, jaki system operacyjny ich obsługuje – bo przecież dla nich istotne jest sprawne działanie programu, który wykorzystują.

Popularność Windows i brak popularności Linuksa na komputerach osobistych wynika po prostu z „woli ludu" i co tu dużo ukryć ze znakomitego dostosowania MS Windows do obsługi przez użytkowników, którzy nie posiadają specjalistycznej wiedzy. Spowodowało to rozpowszechnienie się programów użytkowych dla tego systemu (tak jak kiedyś w USA dla systemu CP/M) i w konsekwencji opanowanie rynku komputerów osobistych. Doszła do tego polityka powszechnego udzielania licencji OEM, w wyniku której większość komputerów osobistych jest oferowana na rynku z systemem operacyjnym MS Windows (choć trafiają się także takie z Linuksem w wersji OEM – np. HP/SuSE Linux).

Jednak póki co na komputerze z Linuksem nie da się zagrać w „Wiedźmina" - a więc nie jest on atrakcyjny jako prezent komunijny lub komputer, którego mamy używać zarówno do pracy, jak i dla rozrywki.

W efekcie mamy do czynienia z efektem zwanym „Vendor Lock-In". Pisałem już o nim sporo – np. w tekście www.aba.krakow.pl/Download/Artukuly/locked_in.pdf . Wykorzystywanie oprogramowania użytkowego dla systemu Windows jest najczęściej związane z koniecznością uiszczenia opłaty licencyjnej. Co więcej zazwyczaj jest ona uzależniona od liczby użytkowników programu. Dla wielu firm oznacza to konieczność ponoszenia znacznych wydatków, a w przypadku użytkowników prywatnych prowadzi często do korzystania z programów użytkowych w sposób niezgodny z prawem. Warto jednak podkreślić, że sytuacja ulega korzystnym zmianom i np. LibreOffice jest dostępne także w wersji dla systemu MS Windows.

Nawet jednak zaprzysięgli zwolennicy MS Windows oraz Linux i posiadania „wszystkiego na moim komputerze" muszą przyznać, że takie (równie ortodoksyjne jak „Linusowych Talibów") podejście rodzi wiele problemów związanych przede wszystkim z ochroną danych. Komputer osobisty (tablet, smartfon itp.) stosunkowo łatwo można utracić w wyniku kradzieży, włamania do samochodu, rozboju – a nawet przypadkowo go pozostawić w taksówce lub pociągu. Konieczna jest również ochrona antywirusowa (chcemy przecież bez większych ograniczeń korzystać z zasobów Internetu) oraz transmisji sieciowych. Warto zestawić dwa fakty – świetna książka Prof. Bliklego „Doktryna Jakości" to około 200 stron PDF oraz 3,4 MB. Na dysku nowoczesnego komputera przenośnego zmieści się więc prawie 100 000 (sto tysięcy!) takich książek! Toż to ogromna biblioteka. Daje to pewne wyobrażenie o ilości danych, które możemy utracić wraz z naszym komputerem lub w przypadku nieodwracalnego uszkodzenia jego twardego dysku.

Lansowanym obecnie rozwiązaniem jest tak zwana chmura. Tak naprawdę oznacza to powrót do starych dobrych czasów, gdy królowały wielkie komputery MainFrame oraz towarzyszące im rozwiązania dostępowe (Front End Processors, Channel Extensions itp.). Podobnie rzecz się ma z wirtualizacją – przecież wywodzi się ona w prostej linii z techniki partycjonowania maszyn IBM, która pozwalała na uruchomienie wielu niezależnych systemów operacyjnych na jednej maszynie fizycznej (np. IBM zSeries z900). Warto podkreślić, że serwer ten otrzymał jako pierwszy certyfikat bezpieczeństwa (Assurance Level) EAL5 Common Criteria (świetna merytoryczna strona o Common Criteria to http://www.cesg.gov.uk/publications/com-crit-itsec.shtml).

Oczywiście rozwiązania proponowane w ramach „chmur" są nieco inne, jednak sama idea jest taka sama – dane pozostają cały czas na odpowiednio zabezpieczonych, profesjonalnie administrowanych serwerach, zaś użytkownicy korzystają ze stacji dostępowych. Kiedyś były nimi terminale – dziś są to głównie komputery PC (lub nowoczesne terminale sieciowe). Wielu z nas już korzysta z różnych chmur – np. poczty elektronicznej gmail, serwisów umożliwiających gromadzenie zdjęć, google documents...

Podnoszone kiedyś obawy o możliwość utraty połączenia sieciowego tracą obecnie znaczenie ponieważ łącza internetowe są coraz bardziej niezawodne i oferowane przez wielu operatorów telekomunikacyjnych. Umożliwiło to praktyczne wprowadzenie w życie starego hasła reklamowego firmy SUN - „Dopiero sieć to komputer".

Decydując się na takie rozwiązanie musimy jednak zaufać dostawcy usług, że należycie zabezpieczy powierzone mu dane. Oczywiście poziom wymaganych atrybutów ochrony informacji: dostępności, integralności oraz poufności (kłania się norma ISO/IEC 27001) będzie uzależniony od ich charakteru. Wiele danych firm i organizacji przeznaczonych jest jedynie do użytku wewnętrznego – a więc możemy je powierzać jedynie takim dostawcom usług zdalnych, którzy zagwarantują nam ich odpowiednią ochronę.

Czy (i jak) można pogodzić wykorzystywanie tego komputera pracy zawodowej oraz do celów prywatnych (słuchanie muzyki, oglądanie filmów, przeglądanie Internetu bez ograniczeń, zabawa z grami itp.) unikając równocześnie ryzyk z tym związanych?

Odpowiedź jest dość prosta – należy chronić informację - a więc dane firmy lub organizacji, w której pracujemy. Jeśli dane te będą przesyłane i składowane na naszym komputerze przenośnym (niezależnie od jego rodzaju) to oczywiście będziemy musieli zadbać o jego należyte zabezpieczenie. Niezbędne będą oczywiście zabezpieczenia programowe (poprawnie skonfigurowana zapora sieciowa, oprogramowanie antywirusowe, połączenie VPN oraz szyfrowanie zbiorów dyskowych), jednak nawet po ich zastosowaniu nie możemy zapominać o podstawowej zasadzie, która mówi, że „Nie ma oprogramowania zabezpieczającego sprzęt". Oczywiście problem ten dotyczy każdego urządzenia – niezależnie od tego, czy korzystamy z Windows czy z Linuksa...

A jaka jest codzienna praktyka? Wystarczy rozejrzeć się wokół siebie:

- Ilu użytkowników PC pracuje wykorzystując konto chronione hasłem i o ograniczonych uprawnieniach systemowych?
- Ilu użytkowników wymienia pomiędzy sobą zdjęcia, pliki muzyczne lub po prostu ściąga je z Internetu? Czy nasza ochrona antywirusowa jest naprawdę szczelna?
- Czy naprawdę sprawdziliśmy, czy programy, z których korzystamy są sprawdzone pod względem integralności (podpis!) i pochodzą z zaufanego źródła?
- Czy korzystając z przeglądarki prowadzimy kontrolę uruchamiania skryptów, a nie tylko korzystamy z blokowania reklam?
- Ilu użytkowników PC zdaje sobie sprawę, że sieć VPN nie zabezpiecza przed przesyłaniem plików mogących uszkodzić dane w naszej firmie (korporacji)?
- Czy zabezpieczamy należycie pliki (łącznie z pocztą elektroniczną!) pobrane z serwerów firmowych? Czy dbamy o skuteczne usuwanie na bieżąco niepotrzebnych już informacji?
- Jeśli szyfrujemy dane na dysku, to czy nasz program szyfrujący jest godny zaufania i czy chronimy starannie hasło niezbędne do ich rozszyfrowania? Wpisanie w Google hasła „Excel Password Recovery" daje ponad 4 miliony wyników!

To tylko kilka problemów nad którymi warto się zastanowić, jeśli korzystamy z naszego komputera przenośnego równocześnie do celów prywatnych i służbowych.

Co więc możemy zrobić?

Moim zdaniem jedynym skutecznym rozwiązaniem tego problemu jest po prostu nieprzechowywanie żadnych ważnych danych służbowych na komputerze przenośnym, który wykorzystujemy także do celów prywatnych. I to zapewnia nam idea chmury.

O ile jednak usługi oferowane w Internecie (Gmail, Google Documents itp.) mają charakter publiczny, o tyle dla rozwiązań biznesowych o wiele atrakcyjniej przedstawiają się chmury prywatne. Chmura prywatna różni się od publicznej przede wszystkim tym, że za rozwiązanie odpowiada dział IT będący częścią organizacji, a więc możliwe jest precyzyjne zdefiniowanie odpowiedzialności i zakresu świadczonych usług. Brzmi to dość groźnie, ale w przypadku małych firm rozwiązanie może być oparte nawet o jeden serwer aplikacji firmowych pracujący w trybie wielodostępu.

Najprostszym rozwiązaniem w takim przypadku będzie udostępnianie oprogramowania – czyli model określany jako SaaS (Software as a Service). Użytkownik korzysta z programów udostępnianych mu przez serwer za pośrednictwem odpowiedniego klienta programowego zainstalowanego na jego komputerze osobistym. Nie ma przy tym znaczenia, czy komputer użytkownika jest podłączony do sieci lokalnej czy rozległej.

Istotne jest również udostępnianie użytkownikowi zasobów pamięci umożliwiającej bezpieczne przechowywanie jego danych. Pozostaną one w bezpiecznej lokalizacji (np. w serwerowni firmy) i nie będą narażane w sytuacji, gdy użytkownik będzie korzystał ze swego komputera w celach pozasłużbowych (najczęściej rozrywkowych).

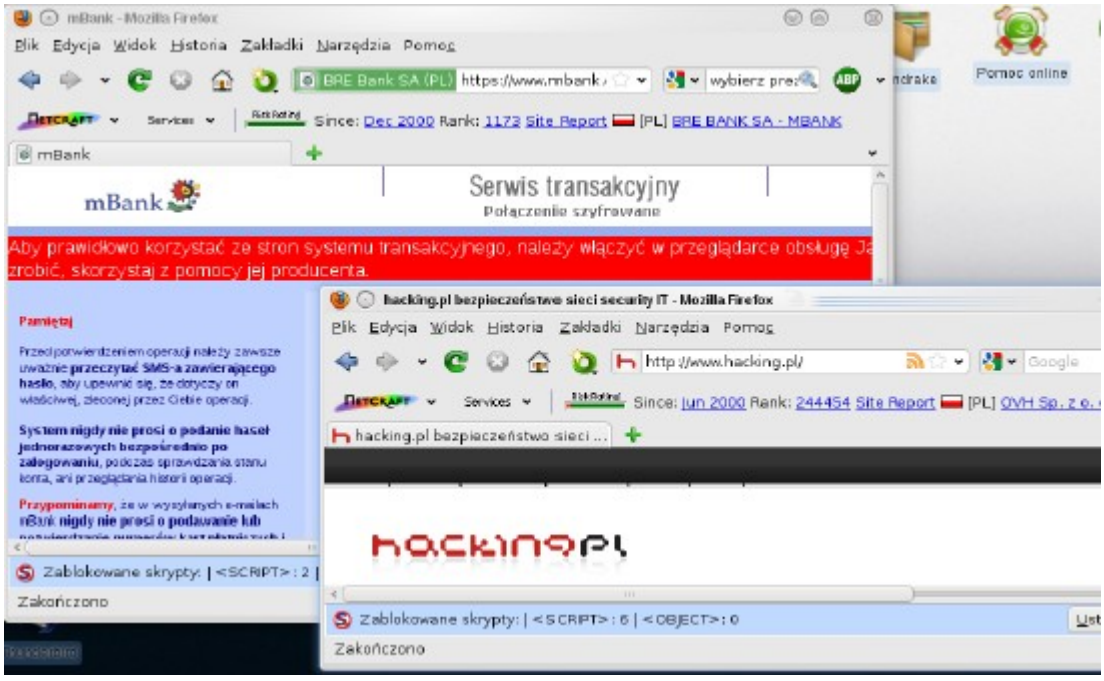
Dalszym krokiem może być wdrożenie funkcjonalności DaaS (Desktop as s Service). Pozwala ona na przeniesienie na komputer użytkownika pulpitu komputera (fizycznego lub częściej wirtualnego) PC umieszczonego w bezpiecznej lokalizacji. Wszystkie zadania służbowe użytkownik wykonuje wówczas na przedzielonym mu komputerze (Blade PC lub na maszynie wirtualnej), zaś jego komputer przenośny jest wykorzystywany jedynie jako urządzenie wejścia / wyjścia.

W obu przypadkach idea rozwiązania zakłada rozdzielenie funkcji „prywatnych" oraz „służbowych" komputera przenośnego. Funkcje „prywatne" są realizowane w taki sam sposób, jak na zwykłym komputerze PC, zaś do realizacji zadań „służbowych" komputer PC jest wykorzystywany jako terminal. Rozwiązanie powinno być niezależne od systemu operacyjnego komputera PC (Windows, Linux, MacOS...) oraz pozwalać na wykorzystywanie dowolnych programów użytkowych eksploatowanych przez firmę. Oczywiście kluczowe jest zagwarantowanie odpowiedniego poziomu bezpieczeństwa takiego rozwiązania.

Chmura prywatna różni się od chmury publicznej przede wszystkim tym, że będą z niej korzystać z niej konkretni (a nie anonimowi) użytkownicy i to za pomocą posiadanych przez siebie komputerów. Opracowując koncepcję chmury prywatnej nie musimy więc troszczyć się o to, aby każdy przypadkowy użytkownik mógł korzystać z jej usług, co jest podstawowym wymaganiem stawianym chmurom publicznym. Ułatwia to znacznie uzyskanie wyższego poziomu bezpieczeństwa, ponieważ:

- zarządzanie nawet znaczną, lecz zdefiniowaną grupą użytkowników jest znacznie prostsze,
- administrator może w bezpieczny sposób (podczas osobistego kontaktu) przekazać uprawnionym użytkownikom wszelkie dane niezbędne do wykorzystywania chmury (oprogramowanie, klucze programowe lub sprzętowe itp.),
- uprawnienia użytkowników mogą być nadawane indywidualne lub w ramach określonych wcześniej ról (Role Based Access Control),
- wykorzystywanie chmury może być monitorowane, zaś w przypadku zgłoszenia utraty sprzętu lub informacji umożliwiających uwierzytelnienie w chmurze dostęp dla konkretnego komputera lub użytkownika może być natychmiast uniemożliwiony.

O ile w chmurach publicznych powszechnie stosuje się przeglądarkę WWW jako uniwersalny interfejs użytkownika (dziś każdy ją ma!) to rozwiązanie to nie wydaje się najkorzystniejszym dla chmur prywatnych. Ilustruje to poniższy zrzut ekranu:



Jak widać, przeglądarka (w tym przypadku Firefox) realizuje równocześnie dwa połączenia – jedno zaufane (https z serwerem banku), a drugie (http) z ogólnie dostępnym serwerem. Proszę również zwrócić uwagę na komunikaty programu NoScript o zablokowaniu skryptów, które oba serwery usiłują przekazać do wykonania na naszym komputerze. Równoczesne realizowanie połączenia zaufanego oraz otwartego przez jeden program (przeglądarkę) nie jest najkorzystniejsze ze względów bezpieczeństwa. Należy także wziąć pod uwagę, że bezpieczeństwo przeglądarki na komputerze osobistym zależy od jej ustawień wprowadzonych przez użytkownika, a zapewne będzie on chciał użyć swego komputera także do połączeń z ogólnie dostępnymi w Internecie serwerami.

Mój entuzjazm do stosowania przeglądarki jako uniwersalnego interfejsu wszędzie, gdzie tylko się da wygasł nieomal całkowicie po tym, jak zetknąłem się z opiniami użytkowników systemów wdrażanych przez jedno z najważniejszych w Polsce ministerstw. Można się z nimi zapoznać na otwartej części forum www.skarbowcy.pl . Oczywiście wiele z sygnalizowanych problemów to mogą być choroby „wieku dziecięcego", ale sama idea „przeglądarki dobrej na wszystko" wydaje się nie sprawdzać w takich instalacjach, choć oczywiście zapewne w chmurach publicznych okaże się nie do zastąpienia.

Korzystniejszym rozwiązaniem wydaje się być technologia wirtualnego pulpitu oczywiście z możliwością publikowania aplikacji. Jak już wspomniałem konieczność instalacji na komputerze użytkownika specjalizowanego klienta programowego w przypadku chmury prywatnej nie tylko nie jest utrudnieniem, ale wręcz ułatwia zarządzanie bezpieczeństwem dostępu do chmury oraz nadzór nad jej wykorzystywaniem.

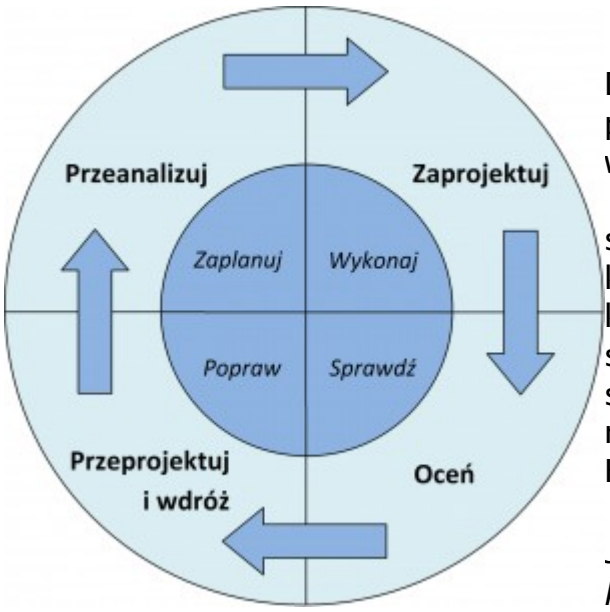
Prywatna chmura musi być bezpieczna. To nie podlega dyskusji. Należy więc zapewnić dostępność, integralność oraz poufność informacji (kłania się norma ISO/IEC 27001). Zarządzanie chmurą (także prywatną) to świadczenie usług IT i nie ma tu znaczenia, że w wielu przypadkach dział zarządzania tymi usługami znajduje się wewnątrz organizacji – warto więc również sięgnąć po normę ISO/IEC 20000 – Information Technology Service Management (niestety, jak na razie nie ma jej polskiej wersji).

Spróbuję określić najważniejsze moim zdaniem wymagania, które powinna spełnić chmura prywatna:

- **Dostęp do systemu oraz uwierzytelnienie:**
  Moim zdaniem powinno obejmować zarówno uwierzytelnienie sprzętu, z którego korzysta użytkownik, jak i oczywiście uwierzytelnienie osobiste. Pierwszym etapem powinno być automatyczne uwierzytelnienie sprzętu na z wykorzystaniem jego cech indywidualnych, systemu kluczy prywatno-publicznych itp. Uwierzytelnienie powinno być obustronne. Dopiero po pozytywnej weryfikacji sprzętu powinno być możliwe uwierzytelnienie osobiste użytkownika. Bezpieczny kanał komunikacji (także w sieci lokalnej) powinien być zestawiony już na etapie uwierzytelniania sprzętu.
- **Integralność oraz poufność informacji:**
  Właściwości te powinien zapewnić zestawiony kanał komunikacyjny. Powinien on być zestawiany wyłącznie z określoną lokalizacją oraz wykorzystywany jedynie do przesyłania informacji wejściowych i wyjściowych (sygnały z klawiatury, myszki, treść do wyświetlenia na ekranie itp.), a nie do przesyłania danych na dysk komputera osobistego. Dzięki temu unika się koegzystencji danych służbowych oraz prywatnych na dysku komputera osobistego (dziś najczęściej przenośnego).
- **Efektywna i bezpieczena praca zarówno w sieci lokalnej jak i rozległej:**
  Założeniem chmury (także prywatnej) jest możliwość korzystania z oferowanych przez nią usług w dowolnym miejscu. Jakże wiele osób korzysta z tych samych komputerów w pracy (po podłączeniu do sieci lokalnej – często bezprzewodowej), w domu (poprzez łącze internetowe) lub w pociągu czy też w zasięgu „Hot Spotów". Wymusza to w praktyce konieczność efektywnej kompresji transmisji oraz jej szyfrowanie.
- **Praca w środowisku graficznym:**
  Pomimo, że do wielu profesjonalnych zadań środowisko znakowe jest absolutnie wystarczające użytkownicy żądają środowiska graficznego. Czasem prowadzi do wręcz do absurdu – np. obsługi formatek baz danych w przeglądarce WWW. Przecież to tak naprawdę środowisko znakowe – a do jego realizacji używa się często maszyny JAVA, samej przeglądarki itd. Razem trzeba w tym celu zainstalować niekiedy ponad 100 MB oprogramowania. Tylko po to, aby wypełniać i przesyłać pola formatek.
- **Skasowanie wszystkich danych (pamięci cache!) po zakończeniu połączenia.**
  Jeśli dane te będą pozostawione (zwłaszcza na dysku) to w przypadku przejęcia kontroli nad naszym komputerem mogą być wykorzystane.

- **Chmurę prywatną powinniśmy dostosować do potrzeb biznesowych organizacji - a nie do oferty i możliwości dostawcy usług.**
  Przecież budujemy ją dla siebie. Rozwiązanie powinno być więc uniwersalne i nie ograniczać projektanta oraz integratora systemu. Chmura prywatna powinna zapewniać połączenie wszystkiego (Windows PC, Linux PC, MacOS, Unix...) ze wszystkim (serwery Windows, Linux, Mac, UNIX, MainFrame...). W ten sposób zapewnimy sobie nie tylko realizację dzisiejszych potrzeb – lecz również spełnimy warunek określany jako „Design for Change". Technologia WWW nie jest jedynym sposobem realizacji tego postulatu - a już na pewno w przypadku chmury prywatnej najbezpieczniejszym i najefektywniejszym!
- **„Fail over" i „Load Balancig"** - ich zadaniem jest realizacja ciągłej dostępności do danych. W systemach, w których wymagana jest ciągłość dostępu stosowanie odpowiednich rozwiązań zapewniających te właściwości jest oczywiste.

Powyżej wymieniłem tylko kilka podstawowych wymagań, które należy spełnić, aby użytkownicy komputerów przenośnych (i innych tego typu urządzeń) mogli w sposób wygodny korzystać z nich zarówno do celów prywatnych, jak i służbowych – a równocześnie zachowane zostały zachowane reguły zarządzania bezpieczeństwem informacji.



Reguły postępowania, które ilustruje Cykl Deminga powinny również obowiązywać podczas opracowywania koncepcji oraz wdrażania systemów informacyjnych.

Niestety, praktyka często jest inna, a należy sobie zdać sprawę, że istotne jest sprawdzenie koncepcji w praktyce i dokonanie ewentualnych korekt. Często przywiązujemy się zbytnio do swych idei i usiłujemy je wdrażać nawet pomimo silnego oporu „materii". Oczywiście, należy również pamiętać o słynnym powiedzeniu Henry Forda I:

Jakbym zapytał moich PT Klientów czego potrzebuję odpowiedzieliby: ***„Szybszego oraz silniejszego konia!"***

I co najważniejsze klienci Henry Forda I mieliby rację. A on sam spełnił on przecież sygnalizowaną przez nich potrzebę – tylko użył innych środków technicznych niż te, do których wszyscy byli wówczas przyzwyczajeni. Warto o tym pamiętać.

Rozpisałem się „ogólnie" - obiecuję wkrótce następny numer, w którym zaproponuję jak konkretnie to można zrobić...