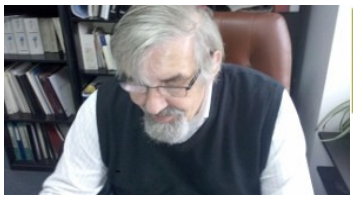

Old Man GURU Magazine

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

Numer 25/2011 14 luty 2012

Coraz więcej mówi się „chmurach". Prawie każdy korzysta już w Google Mail, niektórzy także z innych usług – edycji dokumentów, kalendarza itp. Jednym słowem – chmura publiczna już naprawdę działa. No i bardzo dobrze.

Czy równie szybki postęp następuje w chmurach prywatnych? Wiele osób nie tylko zatrudnionych w firmach IT korzysta z różnego typu komputerów przenośnych oraz połączeń z serwerami zlokalizowanymi w macierzystej instytucji. Są to najczęściej połączenia VPN, zapewniające bezpieczeństwo przesyłanych danych, lecz ich przetwarzanie w przeważającej liczbie przypadków odbywa się na komputerze użytkownika, który pobiera potrzebne mu pliki, a następnie po ich przetworzeniu przesyła z powrotem na serwer firmowy do dalszej obróbki. Nie można tego więc nazwać przetwarzaniem w chmurze.

Stosunkowo rzadko można spotkać użytkowników, którzy korzystają na swych komputerach przenośnych np. ze środowiska wirtualnego desktopu lub innych rozwiązań umożliwiających wykorzystywanie programów użytkowych pracujących na maszynach (fizycznych lub wirtualnych) zainstalowanych w siedzibie firmy lub urzędu.

Uzasadnione jest więc pytanie, czy wdrożenie chmury prywatnej może przynieść rzeczywiste korzyści?

Bezpieczeństwo informacji

Ideą przetwarzania w chmurze prywatnej jest składowanie i przetwarzanie danych na komputerach znajdujących się w siedzibie organizacji. Komputery te mogą być należycie zabezpieczone fizycznie w serwerowniach wyposażonych w systemy kontroli dostępu. Zabezpieczenia programowe możemy powierzyć specjalistom i nie będą one (jak w przypadku klasycznych komputerów PC) zależne od woli i wiedzy użytkowników.

Pliki zawierające istotne dla organizacji informacje nie opuszczają jej siedziby – z zasady nie są przesyłane na komputery użytkowników (za wyjątkiem przypadków, w których jest to absolutnie niezbędne). Zapobiega to ich upublicznieniu – zarówno przypadkowemu, jak i zamierzonemu.

Pliki użytkowników są składowane na dyskach komputerów zainstalowanych w siedzibie organizacji, co znacznie ułatwia organizację systemu kopii awaryjnych (backups) oraz przyspiesza proces odtwarzania danych w razie wystąpienia takiej potrzeby.

Kontrola oprogramowania

Użytkownicy mogą korzystać jedynie z takiego oprogramowania, które zostało im udostępnione w chmurze. Znakomicie ułatwia to kontrolę licencji dzięki redukcji do minimum oprogramowania instalowanego na komputerach PC.

Elastyczność

Wbrew potocznej opinii wykorzystywanie środowiska chmury prywatnej zapewnia bardzo dużą elastyczność. Użytkownik może korzystać z programów użytkowych pracujących na różnych serwerach, niezależnie od ich systemu operacyjnego – tak w trybie publikacji desktopu, jak i poszczególnych aplikacji.

Wprowadzenie nowych użytkowników może być realizowane bardzo szybko.

Centralizacja zarządzania

Wykorzystanie centralnego systemu zarządzania kontami i uprawnieniami użytkowników chmury (np. przy użyciu LDAP), integracja przestrzeni dyskowej na serwerach typu NAS, wirtualizacja serwerów, hostów, a nawet komputerów PC ułatwiają znacznie zarządzanie infrastrukturą IT.

Należy przy tym pamiętać, że ze środowiska chmury prywatnej można z powodzeniem korzystać także w sieciach lokalnych! Dzięki tej właściwości możemy w firmie kontynuować prace rozpoczęte w domu i odwrotnie.

Zapytałem kilka osób ze środowiska IT, dlaczego tak rzadko korzysta się z tej możliwości i czy planują wdrożenie środowiska chmury prywatnej. W większości były to osoby z firm korzystających już z wirtualizacji serwerów, a nawet ze środowiska usług terminalowych serwerów MS Windows. Typowe odpowiedzi były następujące:

- Nasi użytkownicy często pracują poza firmą i wykorzystują przenośne nośniki danych (popularne PenDrive), muszą więc i tak dysponować lokalnym oprogramowaniem na swych komputerach.
- Połączenia internetowe nie są na tyle pewne, aby można je wykorzystywać do ciągłej pracy.
- Praca w trybie zdalnego lub wirtualnego pulpitu wymaga znacznego pasma sieciowego.
- Praca „on-line” wiąże się ze znacznymi zagrożeniami. Możliwe jest przejęcie sesji lub atak typu „Denial of Service”, który uniemożliwi kontynuowanie pracy.
- Trudno jest skutecznie rozwiązać problemy ochrony dostępu – użytkownicy nie przykładają należytej wagi do zarządzania swymi hasłami.

Ze środowiska chmury prywatnej korzystam już od dłuższego czasu. Udało mi się również wdrożyć kilka (niezbyt wielkich) tego typu rozwiązań, postaram się podzielić

praktycznymi uwagami dotyczącymi budowy takiego środowiska i odpowiedzieć na powyższe wątpliwości:

Problem przenośnych nośników USB:

Rzeczywiście, coraz powszechniej korzystamy z przenośnych nośników danych podłączanych do portów USB. Na rynku jest szereg miniaturowych nośników o znacznych pojemnościach (kilkanaście GB), zaś mniejsze (4 GB) stały się popularnymi gadżetami reklamowymi rozdawanymi za darmo przy okazji różnych imprez. Proste użytkowanie powoduje, że użytkownicy wywierają znaczną presję na działy IT, aby korzystanie z tych nośników było nie tylko możliwe, ale i jak najłatwiejsze.

Korzystanie z tych nośników trudno jednak uznać za bezpieczne, ponieważ zazwyczaj zawierają one nieszyfrowane informacje i mogą zostać bardzo łatwo zagubione oraz skradzione. Szyfrowanie danych składowanych na nośnikach przenośnych poprawia oczywiście poziom bezpieczeństwa (jeśli korzystamy ze sprawdzonego algorytmu – np. AES) oraz we właściwy sposób zabezpieczymy dostęp do kluczy. Nie zmniejsza to jednak zagrożenia związanego z utratą danych wraz z nośnikiem.

Na stronach National Security Agency (www.nsa.gov) w poradach dotyczących bezpiecznej konfiguracji systemów operacyjnych (MS Windows, Linux oraz MacOS) zalecane jest wyłączenie obsługi urządzeń USB Storage (PenDrive, telefony komórkowe, aparaty fotograficzne itp.):

2.2.2.2 Disable USB Device Support

USB flash or hard drives allow an attacker with physical access to a system to quickly copy an enormous amount of data from it.

Jeśli więc kopiowanie danych z wykorzystaniem nośników przenośnych jest nam rzeczywiście niezbędne, to musimy zadbać o fizyczne zabezpieczenie komputera przez dostępem osób niepowołanych, co w wielu przypadkach jest iluzoryczne lub wręcz niemożliwe.

Połączenia internetowe

Łącza o prędkości powyżej 1 Mbps stały się już powszechne. Prędkość ta jest oczywiście niezbyt zadowalająca dla transmisji dużych plików (poniżej 100 kB/s). Inaczej wygląda sytuacja w przypadku przesyłania treści ekranu. Przy rozdzielczości 1024x768 oraz 16 bitowej głębi kolorów (wartości w pełni wystarczające dla typowej pracy biurowej) przesłanie całego ekranu (poniżej 1 Megapixeli) nie powinno zająć więcej czasu niż kilkanaście sekund. Jednak należy wziąć pod uwagę, że sytuacja, w której w taki sposób musimy przesłać treść obrazową występuje stosunkowo rzadko. Nowoczesne protokoły są wyposażone w efektywne mechanizmy kompresji oraz obsługę pamięci notatnikowych, co powoduje znaczną redukcję wymagań komunikacyjnych. Na przykład w pełni komfortowe korzystanie ze zdalnego programu biurowego OpenOffice 3.2 na systemie Ubuntu nie wymaga pasma powyżej 1 Mbps. Nawet korzystając z programów graficznych (np. Gimp) dysponując łączem internetowym 1-2 Mbps nie odczujemy wpływy ograniczenia pasma

sieci. Oczywiście jeśli chcemy oglądać filmy on-line (zwłaszcza w rozdzielczości HD) sytuacja będzie zupełnie inna...

W bardzo prosty sposób możemy sprawdzić w praktyce, czy nasze łącze zapewnia wystarczającą prędkość. Ze strony www.nomachine.com pobieramy program klienta odpowiedni dla naszego systemu (pod zakładką Downloads znajdziemy wersje dla systemów MS Windows, Linux, MacOS i Solaris), instalujemy i łączymy się jako gość z serwerem *testdrive.millenux.com*. Możemy korzystać z OpenOffice, Gimpa oraz innych programów w systemie Ubuntu. Jeśli na naszym komputerze uruchomimy monitor pracy sieci przekonamy się, jak niewielkie pasmo jest potrzebne dla takiej pracy.
(Podobnie można zrealizować połączenie w systemem MS Windows – zarówno pracującym na komputerze wirtualnym, jak i fizycznym).

W tym miejscu zazwyczaj pada kolejne pytanie – no dobrze, ale co się stanie, jeśli w czasie pracy transmisja ulegnie zerwaniu? Otóż transmisja tak, lecz sesja nie (dla NoMachine NX nie dotyczy te sesji użytkownika guest). Po ponownym nawiązaniu połączenia znajdziemy się w tym samym miejscu naszej pracy, w którym ją nam przerwano (lub przerwaliśmy ją sami np. wychodząc do domu).

Zagrożenia sieciowe:

Poprawna konfiguracja chmury prywatnej jest w stanie ograniczyć je do minimum. Warunkiem podstawowym jest oczywiście poprawne skonfigurowanie serwera dostępowego w taki sposób, aby udostępniał jedynie naprawdę niezbędne do pracy usługi. Wyłączanie obsługi niewykorzystywanych protokołów, kontrola poprawności praw dostępu itp. powinny być zawsze przestrzeganą zasadą. Można w tym celu skorzystać z dostępnych w sieci „list kontrolnych" (polecam znów serwer www.nsa.com).

Kolejnym krokiem powinno być wprowadzenie uwierzytelnienia komputerów, które mogą się komunikować z serwerem dostępowym. O ile takie rozwiązanie jest w praktyce niemożliwe (lub przynajmniej kłopotliwe) w przypadku chmur publicznych, to w przypadku chmury prywatnej powinno być regułą. Przypominam – nie chodzi w tym przypadku o uwierzytelnienie osoby, lecz komputera, z którego ona korzysta. Serwer nie powinien odpowiadać na żądania połączenia przesyłane z przypadkowych komputerów. Najczęściej realizuje się to za pomocą systemu kluczy prywatno – publicznych. Klucze powinien wygenerować administrator chmury i zainstalować je na komputerze jej użytkownika dopuszczonego do wykorzystywania chmury. Proces uwierzytelnienia komputera (lub innego sprzętu) powinien być realizowany automatycznie bez udziału użytkownika. Dopiero po pozytywnym uwierzytelnieniu sprzętu użytkownik będzie mógł uzyskać dostęp do systemu - w najprostszym przypadku po wprowadzeniu nazwy (login) oraz hasła. Oczywiście dane te powinny być przesyłane w postaci zaszyfrowanej.

Serwer dostępu nie powinien realizować żadnych innych połączeń (łącznie z protokołem ICMP – czyli np. nie odpowiadać echem na ping), a wszystkie funkcje realizować jedynie

wykorzystując tunelowanie. Jeśli korzystamy z tunelowa SSH (NoMachine NX) powinien być otwarty jedynie port 22 (lub inny wybrany).

Zadaniem serwera dostępowego jest zarządzanie dostępem użytkowników do programów użytkowych (SaaS – Software as a Service) aż do komputerów fizycznych lub częściej wirtualnych (PaaS – Platform as a Service).

Czy chmura się opłaci?

Na koszty instalacji umożliwiającej bezpieczny dostęp w trybie wirtualnego desktopu do infrastruktury IT organizacji składa się koszt serwera (lub w przypadku większych instalacji serwerów) dostępowych, koszt modernizacji (instalacja oprogramowania) komputerów osobistych (ew. cienkich klientów) oraz koszt wdrożenia systemu (konfiguracja środowiska, konsolidacja kont i środowiska użytkowników itp.).

Jednak chmura to nie tylko koszty – ale również znaczne oszczędności. Są one przede wszystkim związane z możliwością wykorzystywania komputerów o mniejszej mocy, ponieważ oprogramowanie użytkowe pracuje na komputerach w siedzibie organizacji. Dzięki temu można znacznie wydłużyć czas eksploatacji komputerów użytkowników lub zastosować tańsze, słabiej wyposażone jednostki o mniejszej mocy obliczeniowej oraz ograniczonych zasobach pamięci (zarówno RAM, jak i dyskowej).
Wprowadzenie chmur prywatnych może znacznie ograniczyć wydatki na zakup nowych komputerów PC. Oszczędności te mogą sięgać nawet ponad 1000 złotych na jedno stanowisko pracy i mam na myśli jedynie koszty zakupu nowego sprzętu.

Jeszcze większe oszczędności można uzyskać na zakupie licencji na korzystanie z oprogramowania. Ceny licencji sieciowych lub wielodostępnych są zazwyczaj niższe niż jednostanowiskowych. Ponieważ rozwiązanie chmury prywatnej umożliwia korzystanie zarówno z systemów rodziny MS Windows, jak i Linux, MacOS oraz Solaris możemy wybrać najkorzystniejszy zestaw programów użytkowych.

Na zakończenie jeszcze jedna bardzo ważna uwaga. Obecnie coraz większa liczba użytkowników korzysta dla celów służbowych z komputerów przenośnych. Lecz nie oszukujmy się – komputery te bardzo często są wykorzystywane równocześnie do celów prywatnych. W rezultacie na ich dyskach znajdują się zarówno pliki stanowiące własność organizacji, dla której użytkownik pracuje oraz pliki prywatne (poczta elektroniczna, zdjęcia cyfrowe itp.). Użytkownicy zazwyczaj nie widzą w tym problemu wyjaśniając „do połączenia z firmą wykorzystuję jedynie VPN" i nie zastanawiają się przed czym tak naprawdę zabezpiecza ich klasyczne połączenie VPN.
Praca w dobrze skonfigurowanej chmurze prywatnej nie wymaga przesyłania plików z komputera osobistego na serwery organizacji, eliminuje więc skutecznie zagrożenia z tym związane.