Old Man GURU Magazine

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

Numer 14/2011 6 lipiec 2011

O chmurach mówi się coraz więcej. I nie tylko mówi. Możemy już korzystać na przykład z oferty Google – i w zasadzie wystarczy nam do większości zadań przeglądarka. Mamy do dyspozycji pocztę elektroniczną, edytor, arkusz kalkulacyjny, narzędzia do rysowania, przeglądania zdjęć – a więc możemy wykonać większość codziennych zadań bez potrzeby zakupu i instalacji oprogramowania na naszym komputerze.

Pozostaje tylko jeden problem – nasze zdjęcia, dokumenty oraz inne dane są przechowywane „gdzieś w chmurze". Rodzi to wiele wątpliwości potencjalnych użytkowników.

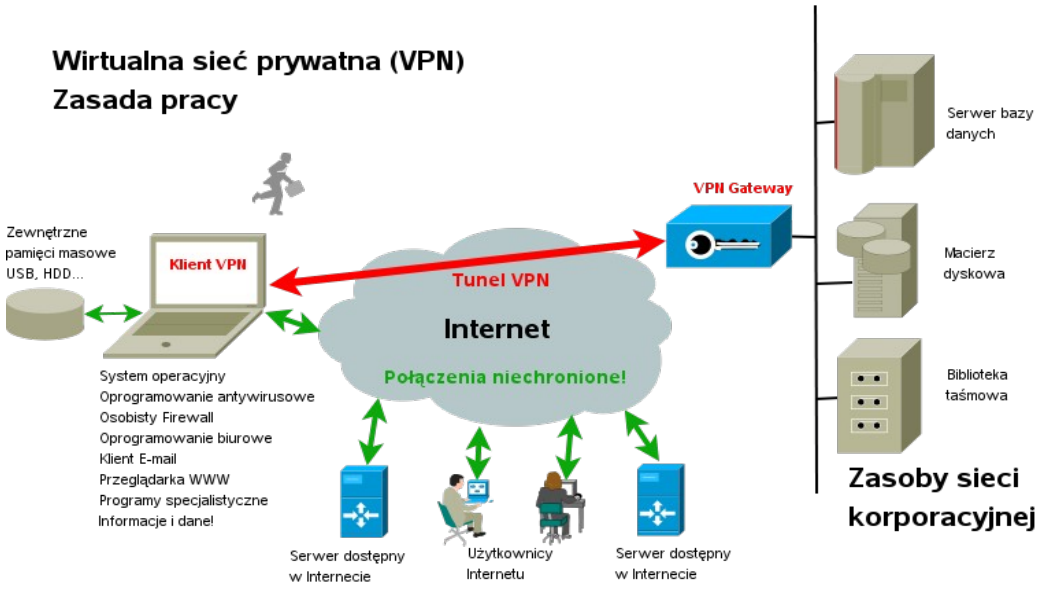
Jednak co w jednym przypadku można uznać za wadę – w drugim może być atrakcyjną zaletą. Mam na myśli rozwiązanie „chmury prywatnej". Pisałem już nieco na ten temat w 12 numerze „Old Man Guru", jednak kilka pytań otrzymanych pocztą oraz zadanych podczas dyskusji zachęciło mnie do kontynuowania tematu.

Przede wszystkim – jaka jest różnica pomiędzy „prywatną chmurą" a typowym rozwiązaniem VPN?

W większości stosowanych w praktyce rozwiązań sieć VPN jest wykorzystywana do utworzenia i zabezpieczenia kanału komunikacyjnego pomiędzy komputerem użytkownika, a siecią firmy lub instytucji. Kanał ten służy do zabezpieczania transmitowanych danych przed „hakerami", jednak najczęściej użytkownik komputera (notebooka, netbooka lub stacji roboczej zainstalowanej w filii lub w domu) korzysta z lokalnego oprogramowania oraz z możliwości składowania danych na lokalnym dysku lub podłączanych pamięci masowych (np. Flash USB). Niektóre rozwiązania oferują nawet tworzenie zdalnych kopii awaryjnych z wykorzystaniem szyfrowanych połączeń VPN.

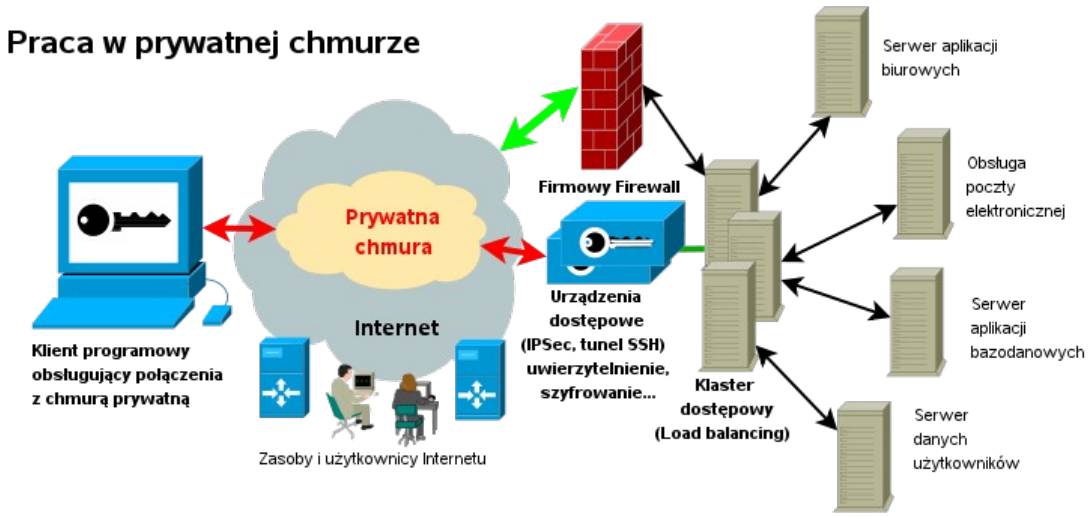
Zaawansowane rozwiązania VPN zapewniają skuteczną ochronę transmisji realizowanych pomiędzy komputerem użytkownika, a siecią korporacyjną, jednakże nie zapewniają np. ochrony komputera przenośnego przed utratą (łącznie z danymi) w wyniku kradzieży. W praktyce większość użytkowników korzystających z VPN może bez problemów wymieniać dane (np. za pomocą popularnych USB PenDrive), przegrywać zdjęcia z aparatów cyfrowych i nowoczesnych telefonów oraz korzystać z ogólnie dostępnych usług Internetu.

Aby to sprawdzić, wystarczy rozejrzeć się wokół! Oczywiście, użytkownicy z pomocą działu IT starają się chronić swoje komputery – ale czy naprawdę ta ochrona może być absolutnie skuteczna? O tym napiszę nieco dalej...



W chmurze jest inaczej.

W chmurze jest inaczej. Zasada pracy w chmurze to wykorzystywanie zdalnego oprogramowania oraz składowanie danych poza własnym komputerem. W przypadku „chmury prywatnej" oznacza to, że użytkownik nie tylko korzysta z oprogramowania zainstalowanego w sieci firmy lub instytucji, lecz również przechowuje swoje pliki na serwerach zainstalowanych w tej sieci. A w chmurze prywatnej maszyny są pod kontrolą administratorów systemów (ASI), bezpieczeństwa (ABI) itp. wykonywane są regularnie kopie awaryjne, opracowane są plany zarządzania ciągłością pracy, procedury awaryjne... Tak więc chmura prywatna nie tylko nie zmniejsza zaufania do zachowania podstawowych atrybutów informacji wymaganych przez normę PN-ISO/IEC 27001, ale wręcz znacznie poziom tego zaufania podnosi!



Praca w prywatnej chmurze różni się znacznie od wykorzystywania klasycznego rozwiązania VPN. Najważniejsze różnice to:

Użytkownik chmury nie wykorzystuje oprogramowania na swoim komputerze.

Uruchamia jedynie program umożliwiający mu dostęp do prywatnej chmury. Może to być program specjalizowany np. klient IPSec, NoMachine NX (tunel SSH) itp. albo (podobnie, jak w chmurach publicznych takich jak Google Documents) przeglądarka WWW wykorzystująca połączenia szyfrowane.

Stacja robocza użytkownika może więc nawet nie zawierać pełnego systemu operacyjnego, a jedynie jego ograniczoną (a więc bezpieczniejszą) wersję typu Embedded, która umożliwia uruchomienie wspomnianego powyżej klienta programowego oraz oczywiście zapewnia obsługę interfejsu użytkownika. Tak więc dostęp do prywatnej chmury może być realizowany nawet z terminala. Firma ABA opracowała w tym celu specjalne wersje oprogramowania swych terminali ABA-X3 dostosowane do pracy w chmurach prywatnych. Są one wyposażone w zaawansowany system uwierzytelniający sprzęt i wykorzystywane na przykład w jednym z bardziej popularnych w Polsce banków.

Oczywiście nic nie stoi na przeszkodzie, aby dostęp do prywatnej chmury uzyskiwać z komputera wyposażonego w pełny system operacyjny – stacjonarnego PC, notebooka lub netbooka, tabletu, a nawet z telefonu komórkowego typu „Smartphone”. Wystarczy jedynie instalacja odpowiedniego dodatkowego oprogramowania.

Na komputerze (teminalu) użytkownika nie są składowane żadne dane.

Ponieważ użytkownik pracuje tak naprawdę, korzystając z oprogramowania (np. Office) zainstalowanego i uruchamianego na serwerze aplikacji, który znajduje się w siedzibie firmy oraz posiada katalog domowy na serwerze danych użytkowników (również w siedzibie firmy) dane nie opuszczają strefy zabezpieczonej fizycznie. Całość transmisji jest szyfrowana, co minimalizuje prawdopodobieństwo ich przechwycenia w sieci, a dostęp uwierzytelniony. Należy jedynie zadbać, aby oprogramowanie kasowało skutecznie pamięć notatnikową (cache) i możemy być pewni, że nawet w przypadku kradzieży naszego komputera dane firmowe nie zostaną upublicznione.

Praca w trybie wirtualnego desktopu.

Jeśli użytkownik wykorzystuje komputer PC zainstalowany w sieci firmowej, może go wykorzystywać także za pośrednictwem prywatnej chmury. Większość nowoczesnych systemów operacyjnych (np. MS Windows czy Linux lub UNIX) obsługuje protokoły umożliwiające zdalne podłączanie się do sesji. Użytkownik może więc kontynuować swą pracę zdalnie, ponieważ połączenie zapewnia odpowiedni poziom bezpieczeństwa. Praca w tym trybie nie różni się w praktyce niczym od pracy na fizycznej konsoli komputera oraz może być także realizowana na maszynach wirtualnych.

Bezpieczne i kontrolowane wykorzystywanie Internetu.

Jednym z większych zagrożeń dla komputerów PC (zwłaszcza przenośnych) jest wykorzystywanie Internetu. Powoduje to konieczność stosowania wielu zabezpieczeń (programy antywirusowe, osobisty firewall, systemy antyspamowe itp.).

Jeśli korzystamy z prywatnej chmury, możemy wykorzystywać łącze firmowe do połączeń z sieciami publicznymi – w tym także Internetem. Wystarczy w tym celu skonfigurować nasz komputer w taki sposób, aby nie mógł on realizować żadnych połączeń za wyjątkiem uwierzytelnianych i szyfrowanych transmisji z chmurą prywatną! Oczywiście, łączymy się z Internetem w dowolny sposób (Neostrada, otwarta sieć WiFi w hotelu lub innym HotSpot), uzyskujemy adres DHCP – ale połączenie możemy zestawić jedynie z naszą prywatną chmurą! Po nawiązaniu połączenia uruchamiamy przeglądarkę (lub inny program) na serwerze aplikacji i łączymy się z Internetem poprzez firmowy bastion Firewall. Bezpośrednie połączenie jest po prostu niemożliwe – możemy nawet nie mieć zainstalowanej przeglądarki. Dzięki takiemu rozwiązaniu możliwe jest ścisłe przestrzeganie Polityki Bezpieczeństwa – także dla pracowników pracujących poza siedzibą firmy. Ochrona przed atakami zewnętrznymi jest realizowana przez fachowców – pracowników Działu IT i skoncentrowana w jednym lub najwyżej kilku punktach dostępu do Internetu. Jak bardzo ułatwia to śledzenie pojawiających się zagrożeń, instalację poprawek, łatek i uzupełnień programów zabezpieczających, aktualizację filtrów antyspamowych nie trzeba chyba nikogo przekonywać. Dowodem, że możliwe jest efektywne zarządzanie taką chmurą, jest choćby znikoma ilość spamu pojawiającego się w poczcie Google (gmail.com).

Prywatna chmura i zarządzanie bezpieczeństwem informacji czyli ISO 27001 itp.

System zarządzania bezpieczeństwem informacji to przede wszystkim rozpoznanie zagrożeń i podatności, kwalifikacja informacji oraz ocena ryzyka i jego znaczenia dla działalności biznesowej.

Normy PN-ISO/IEC 27001 oraz PN-ISO/IEC 17799 (ISO 27002) wprowadzają trzy atrybuty bezpieczeństwa informacji - **dostępność, integralność i poufność**.

Obecnie chyba już nikt nie ma wątpliwości, że informację należy chronić, oraz że ochrona powinna być selektywna. Praktyka związana ze stosowaną od bardzo dawna ochroną informacji niejawnych dostarcza wielu wzorców postępowania. Za jeden z najważniejszych należy uznać prostą zasadę „im mniej kopii danych chronionych – tym lepiej mogą one być ochronione". Praktycy IT często zbyt dużą wagę przywiązują do zabezpieczeń programowych, a przecież tak naprawdę, to nie istnieje oprogramowanie, które potrafi skutecznie chronić sprzęt.

Na zakończenie tego dość obszernego numeru „Old Man GURU" zamieszczam kilka komentarzy związanych z zarządzaniem bezpieczeństwem informacji w chmurze prywatnej, na które być może nie zwraca się w pierwszej chwili uwagi. Uszeregowałem je według atrybutów wykorzystywanych przez normy rodziny ISO 27000.

Dostępność:

Jeśli konsekwentnie korzystamy z prywatnej chmury, wszystkie nasze pliki są przechowywane na dobrze zabezpieczonych (także fizycznie) serwerach, którymi opiekują się fachowcy. Zagrożenie utratą informacji jest więc bardzo niewielkie.

Pojawia się jednak inny problem – niezawodność kanału komunikacyjnego. Jeśli utracimy połączenie sieciowe, to oczywiście stracimy także możliwość pracy, ponieważ nie będziemy dysponować dostępem ani do oprogramowania, ani do danych.

Spróbujmy jednak porównać to ryzyko z ryzykiem utraty danych przechowywanych lokalnie. Zapewne prawdopodobieństwo, że utracimy (najczęściej na pewien czas) połączenie sieciowe jest większe niż utrata (kradzież, pozostawienie w taksówce itp.), komputera przenośnego lub uszkodzenie jego zbiorów dyskowych przez złośliwe oprogramowanie (oczywiście pod warunkiem posiadania aktualnego oprogramowania antywirusowego). Jednak o ile w przypadku pracy w chmurze prywatnej brak połączenia sieciowego oznacza jedynie chwilową utratę dostępu do informacji, to w przypadku lokalnego składowania danych grozi nam bezpowrotna utrata informacji lub jej upublicznienie!

Brak połączenia sieciowego skutkuje również niemożliwością wykorzystywania połączeń realizowanych za pośrednictwem klasycznych sieci VPN – a więc w obu przypadkach nastąpi znaczne ograniczenie w dostępie do informacji.

Problem kradzieży komputerów przenośnych nie jest problemem „wydumanym”. Oto dane dla USA (http://www.laptopmobilesecurity.com/laptop-security-facts.php):

Laptop Theft Statistics

According to the statistics, business travelers lose more than 12,000 laptops per week in U.S. airports and one laptop is stolen every 53 seconds!

According to Safeware Insurance Agency Inc., over 600,000 laptop thefts occur annually, resulting in an estimated $5.4 billion loss of proprietary information.

The FBI notes that 97% of stolen laptops and computers are never recovered.

According to the 2003 Annual Computer Crime and Security Survey, the value of the information in an average notebook is US$250,000.

W Europie i w Polsce również ten problem zaczyna dawać znać o sobie. Specjalistyczny serwis: (http://www.frazpc.pl/artykuly/827341,Ochrona_notebookow_przed_kradzieza.html) podaje:

Z danych udostępnionych w 2009 roku przez Radę Europy wynika, że aż 92% europejskich małych i średnich przedsiębiorstw, których pracownicy korzystają z mobilnych komputerów, poza miejscem pracy doświadczyło kradzieży notebooka.
W Polsce te liczby są mniejsze, lecz, niestety stale rosną. **W 2005 roku ukradziono w naszym Kraju prawie pięć tysięcy komputerów przenośnych**. W 2009 roku liczba skradzionych notebooków przekroczyła już **siedem i pół tysiąca**. Wszystko wskazuje na to, że statystyki za ubiegły rok nie będą wcale lepsze. Poza tym obejmują one jedynie kradzieże, które zostały zgłoszone i zarejestrowane.

Na rynku są dostępne różnego rodzaju zabezpieczenia fizyczne, lecz utrudniają one korzystanie ze sprzętu. Z kolei zabezpieczenia programowe (szyfrowanie dysku) nie zabezpieczają dostępu do danych, lecz (często iluzorycznie!) ich poufność.

Wydaje się, że wartość danych składowanych na przeciętnym komputerze przenośnym w Polsce jest znacznie mniejsza niż szacowana w USA, lecz i w wielu przypadkach jest znacznie większa niż cena samego komputera.

Integralność:

W tym przypadku największe zagrożenie jest związane z wykorzystywaniem komputera do wymiany danych ze znajomymi oraz do korzystania z Internetu. Jakże często obserwujemy wymianę zdjęć wykonywanych aparatami cyfrowymi lub telefonami komórkowymi, albo innych materiałów za pomocą popularnych PenDrive! O instalacji programów pochodzących z nieznanych źródeł nawet nie wspomnę, ponieważ takiego postępowania zabrania praktycznie każda Polityka Bezpieczeństwa.

Korzystanie z powszechnie dostępnych serwerów usług sieciowych, punktów dostępowych, ściąganie i otwieranie załączników do wiadomości przesyłanych pocztą elektroniczną, a nawet korzystanie ze stron WWW (zwłaszcza tych wykorzystujących różne rozszerzenia programowe) to również poważne zagrożenie dla integralności oprogramowania i danych, ponieważ łatwo przy okazji załadować jakiś złośliwy program. Z okazji dziesiątej rocznicy „narodzin" dość prymitywnego wirusa „I love you" warto przypomnieć, że nie wykrywał go żaden ówczesny program antywirusowy:

"Do tej pory nie widzieliśmy niczego podobnego" - wspomina Paul Fletcher, w owym czasie zatrudniony w firmie Message Labs (cytat za IDG.pl).

Pomimo wysiłków programistów zatrudnionych w firmach tworzących programy zabezpieczające nie ma żadnej gwarancji, że taka sytuacja się nie powtórzy.

A przecież nie czarujmy się: praktycznie każdy komputer, który jest wykorzystywany do komunikacji z siecią firmową, za pomocą połączenia VPN jest także używany do bezpośrednich połączeń z Internetem jako stacja multimedialna!

Ryzyko utraty integralności danych oraz oprogramowania należy więc ocenić jako znaczne. Istotne jest także ryzyko, że ingerencja wrogiego programu (lub osoby) pozostanie niezauważona. O ile bowiem „hakerzy" dbają o to, aby ich działalność była zauważana – o tyle cyberprzestępcy (podobnie jak zwykli przestępcy) starają się zacierać za sobą wszelkie ślady! Warto zdać sobie sprawę, że np. plik zawierający zmienione przez cyberprzestępcę dane zostanie z naszego komputera przekazany (oczywiście w sposób bezpieczny!) przez sieć VPN na serwer firmowy, a na podstawie otrzymanych od nas danych mogą zostać podjęte istotne decyzje.

Poufność:

Zachowanie poufności wydaje się, być proste – wystarczy po prostu zaszyfrować wszystko, co się da. Ale często daje to złudne poczucie bezpieczeństwa – poufność nie gwarantuje bowiem dostępności, a i z integralnością może być różnie (w zależności od algorytmu szyfrowania).

Często spotykam się z twierdzeniem – ja szyfruję wszystkie zapisywane na moim komputerze dane, a więc mogę je traktować jako poufne. Tymczasem specjaliści (Peter Gutmann) ostrzegają przed bardzo niebezpieczną iluzją bezpieczeństwa, jaką często skutkuje szyfrowanie plików. Wystarczy przeszukać sieć – nawet tylko w języku polskim, aby znaleźć mnóstwo darmowych oraz płatnych programów do „odtwarzania" haseł. Fraza „Password breaker" wpisana w wyszukiwarkę Google daje ponad 5 milionów odnośników!

Jeśli więc ktoś uzyska dostęp do komputera z zaszyfrowanymi danymi na dłuższy czas, będzie miał najprawdopodobniej dość czasu, aby podjąć szereg prób odczytania informacji. Nie można więc w żadnym przypadku uważać, że zaszyfrowanie pliku za pomocą standardowych mechanizmów zapewni skutecznie jego poufność.

Na następnej stronie podaję kilka reklam programów do łamania haseł. Znalazłem je w ciągu kilku minut za pomocą niezawodnego Google:

Program radzi sobie bardzo dobrze z dekodowaniem haseł/loginów z takich aplikacji jak Firefox, Thunderbird, Opera, Internet Explorer (wersja 7 i 8), Tlen, Nowe Gadu-Gadu, Gadu-Gadu (starsze edycje i najnowsza 10), AQQ, Microsoft Access, Total Commander, TheBat!, MSN Live Messanger, Gmail Notifier, Google Chrome, a także połączeń Dial-Up i kluczy systemowych.

Program XXX realizuje wydajne rozproszone odzyskiwanie haseł dla agencji sądowych i rządowych, firm świadczących usługi odzyskiwania haseł i danych. Odzyskiwanie nawet najbardziej złożonych haseł i silnych kluczy szyfrowania w rozsądnym czasie.

FirePasswordViewer to narzędzie do odzyskiwania haseł logowania przechowywanych przez Firefoksa. Podobnie jak inne przeglądarki, Firefox przechowuje także hasło, takie jak nazwa użytkownika, hasło dla każdej strony odwiedzane przez użytkownika za zgodą użytkownika. Wszystkie te tajne dane są przechowywane w Firefox bezpiecznie w postaci zaszyfrowanej. FirePasswordViewer może błyskawicznie rozszyfrować i odzyskać te tajemnice, nawet jeśli są zabezpieczone hasłem głównym.
…
Bardzo przydatny, darmowy program, który odzyskuje hasła arkuszy kalkulacyjnych XLS, które zostały stworzone w programie Microsoft Excel 97, 2000, XP i 2003. Aplikacja jest bardzo łatwa w obsłudze nawet dla początkujących użytkowników.

No dobrze, ale co to wszystko ma wspólnego z chmurą – i to do tego w dodatku prywatną?

Otóż, jeśli wybierzemy korzystanie z chmury, to przechowywanie danych na komputerze osobistym staje się po prostu zbędne! Nie ma więc właściwie problemu z ich ochroną, choć oczywiście należy zachować ostrożność i korzystać z uwierzytelnianego oraz szyfrowanego połączenia. Warto też zwrócić uwagę, że zarówno przeglądarki, jak i inne programy (np. klient NoMachine NX) wykorzystują pamięć masową (dysk twardy lub półprzewodnikowy) jako pamięć notatnikową (cache) – należy więc zadbać o to, aby po zakończeniu połączenia była ona automatycznie kasowana. Można to zrealizować za pomocą odpowiedniego programu wsadowego, albo wykorzystać RAM dysk (co dodatkowo zapewni szybszą pracę).

Najistotniejszą zaletą pracy w prywatnej chmurze jest możliwość bezpiecznego korzystania z Internetu.

Komputery (stacjonarne lub przenośne albo wręcz terminale) łączą się jedynie w obrębie prywatnej chmury za pomocą zabezpieczonych (uwierzytelnienie sprzętu i użytkownika, szyfrowanie transmisji) z siecią firmową. Połączenie z Internetem może być realizowane jedynie za pośrednictwem firmowego bastionu firewall. Cały zewnętrzny ruch sieciowy jest więc kontrolowany w jednym punkcie, co znacznie ułatwia tworzenie i wdrożenie Polityki Bezpieczeństwa oraz likwiduje niebezpieczeństwa związane z bezpośrednim podłączeniem komputera do Internetu. Należy podkreślić, że ogranicza to możliwości użytkowników jedynie w takim stopniu, jaki wynika z przyjętej Polityki Bezpieczeństwa.

Osobiście uważam, że „prywatne chmury” mogą być znakomitym rozwiązaniem dla wszystkich organizacji posiadających strukturę rozproszoną (niewielkie oddziały, filie, punkty obsługi klienta) oraz wykorzystujących pracę zdalną i mobilną. Zapewniają one znacznie większe bezpieczeństwo informacji i danych.

Oczywiście, zapewne wielu użytkowników przyzwyczaiło się do ogromnej swobody, jaką zapewnia im służbowy komputer przenośny bez ograniczeń wykorzystywania go do celów pozasłużbowych. Chmura prywatna może wymusić znaczną dyscyplinę, która zapewne przez wielu nie będzie powitana z radością. Jednak coraz częściej okazuje się, że unikaniu ryzyk związanych z naruszeniami zasad ochrony informacji należy nadać najwyższy priorytet.