Teresa Mendyk-Krajewska, Zygmunt Mazur, Hanna Mazur

Konkurencyjność rozwiązań wirtualnych infrastruktury informatycznej

Ekonomiczne Problemy Usług nr 113, 262-271

2014

operacyjnych. Cechuje ją wiele praktycznych zalet, dlatego w ostatnim okresie obserwuje się coraz większe zainteresowanie wykorzystaniem tego środowiska. Liczba firm podejmujących się wirtualizacji swojej infrastruktury systemowej stale rośnie. Równolegle pojawiają się narzędzia umożliwiające proaktywne monitorowanie takich środowisk, zarządzanie nimi i zabezpieczanie danych.

Rozwiązania wirtualne cechują się też pewnymi wadami, które wiążą się ze spadkiem wydajności systemu – obniżeniem mocy obliczeniowej komputera i przepustowości kanałów transmisyjnych. Najwięcej kłopotów może jednak (z różnych przyczyn) sprawiać ochrona tych środowisk przed zagrożeniami sieciowymi. Jeszcze inne problemy dotyczą bezpieczeństwa obliczania w chmurze, dla którego wirtualizacja stanowi podstawę.

Celem artykułu jest ukazanie atrakcyjności rozwiązań wirtualnych infrastruktury informatycznej dla zastosowań w gospodarce elektronicznej, przy jednoczesnym podkreśleniu problemów dotyczących bezpieczeństwa takich środowisk i wskazaniu nowych możliwości ich ochrony.

1. Koncepcje wirtualizacji i maszyny wirtualne

Wirtualizacja jest to „osiągnięcie logicznego zasobu przez abstrakcję zasobów fizycznych" (Porowski 2011). Maszyna wirtualna (*virtual machine*, VM) to wirtualne środowisko dla działania programów, które posiada pełną kontrolę nad wszystkimi wirtualizowanymi zasobami. Cechuje się odizolowaniem (dzięki wprowadzeniu warstwy abstrakcji między sprzętem a oprogramowaniem), zmniejszeniem złożoności struktury i eliminacją redundancji. Maszyna wirtualna nadzoruje wszystkie odwołania aplikacji do sprzętu lub systemu operacyjnego, umożliwiając jej obsługę (Serafin 2011).

Wirtualizacja pozwala w efektywny sposób wykorzystać istniejący sprzęt danego środowiska informatycznego, poprzez modyfikowanie cech wirtualizowanych zasobów zgodnie z potrzebami użytkownika.

Definiowane są trzy architektury programowe wirtualizacji VMM (*Vitual Machine Manager*):

- native VMM (hypervisor typu 1),
- OS-hosted VMM (hypervisor typu 2),
- hybrydowy VMM.

W rozwiązaniu pierwszym hipernadzorca[2] jest uruchamiany bezpośrednio na platformie sprzętowej, nie zależy od nadrzędnego systemu operacyjnego, znajduje

[2] Hiperwizor, narzędzie monitorujące środowisko wirtualne, mające pełną kontrolę nad systemem, instalowane bezpośrednio na fizycznym sprzęcie.

się pomiędzy sprzętem a systemami operacyjnymi gości[3] (Guest-OS). Zaletą jest duża szybkość działania, ze względu na skrócenie ścieżki przepływu żądań między systemem gość a urządzeniami wejścia/wyjścia. Zestaw sterowników danej platformy dostarczany jest wraz z hipernadzorcą. Reprezentantami tego typu są Citrix XEN, Microsoft Hyper-V oraz VMware ESX.

OS-hosted VMM pracuje pod kontrolą standardowego systemu operacyjnego jak zwykła aplikacja. System gość działa w trybie użytkownika maszyny rzeczywistej i m.in. upoważniony jest do swobodnego dostępu do pamięci RAM. Żądania systemu gość są obsługiwane przez proces ULM (*User Level Monitor*, uruchamiany jako proces systemu gospodarza[4]) udostępniający modele wirtualnych urządzeń wejścia/wyjścia. Emulowane są tu elementy maszyn wirtualnych, których nie da się zrealizować ani sprzętowo, ani bezpośrednio w systemie gospodarza. Największą wadą tego rozwiązania jest całkowita zależność hipernadzorcy od systemu gospodarz, a zaletą – łatwość przenoszenia VMM w zakresie innych systemów gospodarz. Realizacje tego typu to najczęściej produkty niby-desktopowe, przykładem może być Virtual Box firmy Oracle.

Trzeci rodzaj architektury – hybrydowy VMM, jest połączeniem dwóch opisanych koncepcji i wykorzystuje ich zalety. Cechuje go używanie sterowników urządzeń wejścia/wyjścia dostarczanych z bazowym systemem operacyjnym.

Środowisko wirtualne obejmuje wszystko, co odnosi się do wirtualnego hosta, także pośrednio. Typowa jego budowa to platforma sprzętowa (host 1 lub host 2), na której uruchamiane są instancje wirtualne (goście), warstwa komunikacji i przestrzeń dyskowa. Istnieją różne koncepcje wykorzystania technologii wirtualizacji, która może dotyczyć serwerów, pamięci operacyjnej, przestrzeni dyskowej, sieci, stacji roboczych i wielu innych. Do popularnych technik wirtualizacji należą: technika wirtualizacji pamięci i wirtualizacja sprzętu komputerowego w celu jednoczesnego funkcjonowania kilku systemów operacyjnych.

Aplikacje do wirtualizacji są ciągle udoskonalane, co przyczynia się do większego zainteresowania nowymi możliwościami. Na rynku wirtualizacji znaczącą rolę odgrywają firmy VMware, Microsoft i Oracle, a w ostatnich latach do rozwoju tej technologii przyczynili się także najwięksi producenci procesorów (Intel, AMD). Dostępnych jest wiele maszyn wirtualnych dla różnych systemów gospodarzy i gości; niektóre są udostępniane bezpłatnie.

Szereg produktów różnej funkcjonalności oferuje będąca liderem firma VMware, wśród nich: VMware vSphere (zbiór aplikacji do zarządzania procesem wir-

---

[3] System gość (*guest operating system*) – system zainstalowany na wirtualnej maszynie; definiowany też jako proces uruchamiany w systemie gospodarz; dysk twardy występuje tu często jako plik o specjalnym formacie (na dysku systemu gospodarz lub zewnętrznej macierzy dysk.).

[4] System gospodarz (*host operating system*) – główny system operacyjny zainstalowany bezpośrednio na fizycznej maszynie, na którym instalowane jest środowisko wirtualne; gdy na fizycznym sprzęcie instalowane jest narzędzie służące tylko do wirtualizacji, termin ten zastępowany jest określeniem hipernadzorca.

tualizacji i zapewniania ciągłej dostępności zasobów), VMware ESXi (darmowy hipernadzorca głównie przeznaczony dla wirtualizacji serwera), a także bardziej rozbudowana wersja komercyjna ESX oraz VMware Server – darmowe rozwiązanie do wirtualizacji serwerów, deskotopów i stacji roboczych. Oprócz wymienionych, firma oferuje też wiele innych narzędzi do różnych zadań (VMwere Workstation, -Converter, -Player, -Fusion i vCloud).

Na uwagę zasługuje Oracle Virtualbox – aplikacja o dużych możliwościach (wiele trybów pracy sieci, emulacja wielu urządzeń, obsługa systemów 64-bit. na procesorach 32-bit. itd.) – typowy hostowy hipernadzorca do wirtualizacji desktopów i stacji roboczych. Narzędzie jest stale rozbudowywane. Przykładowo, wersja 4.2 wprowadza szereg nowych rozwiązań, na przykład możliwość zmiany parametrów maszyny podczas jej pracy czy uruchamianie w trakcie startu systemu.

Innym popularnym hipernadzorcą jest XenServer (XenSource przejęła firma Citrix), który działa tylko w trybie parawirtualizacji[5]. Zarządzanie zasobami odbywa się tu poprzez uprzywilejowaną domenę mającą bezpośredni dostęp do fizycznego sprzętu (zarządza ona także innymi domenami, którym przydzielane są wirtualne zasoby). Wersję XenServer 6 przeznaczoną dla realizacji chmury obliczeniowej cechuje usprawnienie mechanizmów zabezpieczeń.

Bogatą ofertę stworzyła też firma Microsoft (Hyper-V, Virtual PC); na rynku są też dostępne produkty wielu innych dostawców na przykład Red Hat, Parallels.

Według raportu firmy Gartner z czerwca 2012 r. (Bittman 2012) o mocnej pozycji firmy Microsoft na rynku oprogramowania do wirtualizacji decyduje rozbudowane środowisko administracyjne, które używane jest głównie w małych przedsiębiorstwach. Silna pozycja firmy VMware wynika z opracowania systemu vSphere 5.0, dostarczającego kompletny zestaw narzędzi wspomagający hybrydowe i prywatne chmury obliczeniowe.

2. Wirtualizacja dla potrzeb rozwoju gospodarki elektronicznej

Coraz większe zainteresowanie rozwiązaniami wirtualnymi spowodowane jest redukcją kosztów związanych z wdrożeniem i eksploatacją systemów informatycznych oraz optymalnym wykorzystaniem posiadanych zasobów. Możliwość uruchomienia na jednym komputerze (serwerze) kilku maszyn wirtualnych (z wykorzystaniem macierzy dyskowej) oraz łatwość sporządzania kopii zapasowych i szybkość odtwarzania systemu po awarii (przeniesienie środowiska pracy trwa minuty) – to niezaprzeczalne zalety wirtualnych rozwiązań. Ważnymi cechami są też elastyczność konfiguracji zasobów i scentralizowane zarządzanie. Wirtualizacja

[5] Możliwość występowania jednej lub wielu maszyn wirtualnych obok systemu gospodarz (wykorzystywany hipernadzorca typu 1, który jest uruchamiany na sprzęcie); zaletą techniki jest stosunkowo duża wydajność osiągnięta m.in. drogą pominięcia emulacji sprzętu (Wojtczak 2008).

to także możliwość tworzenia zamkniętych środowisk desktopowych przeznaczonych do specyficznych zadań, w tym testowania nowych rozwiązań. „Dociążenie" posiadanych serwerów aplikacjami z innych maszyn oznacza też mniejsze zużycie prądu przez komputery i systemy chłodzenia. Wirtualne maszyny mogą być przesuwane z jednego środowiska do drugiego – w zależności od dostępności zasobów czy obciążenia systemu.

Popularyzacji rozwiązań wirtualnych sprzyja obserwowane w ostatnim okresie (w Polsce i na świecie) spowolnienie gospodarcze, wymuszające ograniczanie wydatków także w obszarze infrastruktury informatycznej. Coraz więcej firm (szczególnie małych i średnich) czerpie korzyści z przeniesienia swojej infrastruktury w środowisko wirtualne. Wzrost wdrożeń środowisk wirtualnych w sektorze MŚP[6] w 2012 r. (w stosunku do 2011 r.) szacowano na 21%, zaś dla dużych przedsiębiorstw wartość ta wynosiła jedynie 14% (Adelberger 2012).

Wirtualizacja serwerów to dla wielu firm optymalna metoda na oszczędność przestrzeni w serwerowni oraz maksymalizację efektywności, zatem staje się ona zjawiskiem dość powszechnym. Interesujące rozwiązanie dla wielu organizacji stanowi też wirtualizacja desktopów umożliwiająca efektywne zarządzanie użytkownikami końcowymi w odległych działach (riverbed.com 2012). W lutym 2010 r. opublikowano wyniki badań ankietowych wykonanych przez firmę Vanson Bourne na zlecenie Citrix Systems, według których do 2014 r. oszczędności działów IT w efekcie wdrożenia technologii wirtualnych wyniosą prawie 30% (Citrix 2010). Ankietą objęto 700 dyrektorów IT z pięciu krajów: Japonii, Kanady, Stanów Zjednoczonych, Niemiec i Wielkiej Brytanii.

Dla ułatwienia administrowania złożonym systemem i monitorowania parametrów pracy poszczególnych instancji maszyn wirtualnych opracowuje się dodatkowe narzędzia. Jednym z nich jest platforma FortiManager, która umożliwia zarządzanie zarówno urządzeniami fizycznymi, jak i maszynami wirtualnymi. Narzędzie FortiAnalyzer służy do zapisywania zdarzeń, raportowania i archiwizacji informacji dotyczących bezpieczeństwa, inne produkty firmy Fortinet[7] pozwalają m.in. dokonać podziału sieci na oddzielne domeny wirtualne (przeznaczone na przykład dla różnych klientów usługodawcy lub jednostek organizacyjnych firmy). Fortinet dostarcza też zintegrowaną platformę bezpieczeństwa (FortiGate), która realizuje szereg funkcji ochronnych i jest jej sztandarowym produktem.

Wiele organizacji dążąc do zwiększenia efektywności przy jednoczesnej redukcji kosztów wykorzystuje technologie chmurowe. Zazwyczaj ogromna liczba przetwarzanych przez organizację (przedsiębiorstwo, firmę) danych (wymagających konsolidacji i sprawnego zarządzania) nadal wzrasta – stąd coraz większe zaintere-

---

[6] Małe i średnie przedsiębiorstwa.

[7] Amerykański producent kompleksowych systemów bezpieczeństwa IT.

sowanie firm przeniesieniem ich do chmury. Równolegle rośnie liczba narzędzi i usług umożliwiających realizację takich zamierzeń.

Cloud Computing (przetwarzanie w chmurze), którego podstawę stanowi wirtualizacja jest jedną z najszybciej rozwijających się technologii informatycznych. Korzysta z niego wielki biznes, coraz bardziej interesują się nim średnie i małe firmy. Klientom oferuje się nowoczesną, rozproszoną infrastrukturę informatyczną, której funkcjonalność dostosowana jest do ich oczekiwań, a koszty obejmują jedynie wykorzystane zasoby i usługi. Różne rozwiązania środowisk chmurowych mają swoje zalety i wady, zatem decyzja o ich wyborze jest zależna od specyfiki organizacji oraz wykorzystywanych przez nią usług. Dla firm, które chcą szybko wprowadzić na rynek usługi bez inwestowania we własną infrastrukturę sprzętową, dobre rozwiązanie stanowi chmura publiczna[8] (potencjalne problemy z płynnym dostarczaniem usług mogą wynikać z dużych opóźnień lub awarii w sieci rozległej). Dla tych, którym szczególnie zależy na bezpieczeństwie i prywatności – lepszą opcją jest chmura prywatna (wykorzystująca wewnętrzną infrastrukturę informatyczną firmy). Na pewno decyzja o umieszczeniu danych i usług poza siedzibą firmy nie należy do łatwych.

Na rozwój technologii przetwarzania w chmurze wpływa różnorodność zastosowań. Nowoczesne centrum danych w Dublinie (pierwsze stworzone przez Microsoft poza USA, podłączone do Internetu w lipcu 2009 r.) jest nadal rozbudowywane, by mogło sprostać rosnącemu popytowi na usługi w chmurze. Jest przykładem zaangażowania firmy Microsoft w ochronę środowiska i stanowi wzór realizacji polityki Unii Europejskiej w zakresie ograniczania zużycia energii elektrycznej.

3. Usługi chmury obliczeniowej

Cloud Computing bazuje na wykorzystaniu wielkiego potencjału serwerów. Umożliwia użytkownikowi dostęp do ogromnej mocy obliczeniowej i niemal nieograniczonej przestrzeni dyskowej, przy jednoczesnej gwarancji użytkowania aktualnej platformy programistycznej. Zalety świadczącego usługi centrum danych to możliwość skonfigurowania serwerów wirtualnych zależnie od własnych potrzeb oraz opcja dzierżawy całego fizycznego serwera, przy pełnej nad nim kontroli. Ponadto centrum danych może dysponować przestrzenią serwerowni na umieszczenie w niej infrastruktury klientów, co rozwiązuje wiele ich problemów (bezpieczeństwo, wsparcie techniczne, konserwacja sprzętu itp.).

Motywacje implementowania chmury prywatnej i wykorzystywania chmury publicznej są różne. W pierwszym przypadku, dzięki grupowaniu zasobów oraz

[8] Dostęp do usług i infrastruktury znajdujących się na zewnątrz firmy możliwy jest poprzez Internet.

dynamicznemu ich przydzielaniu i zwalnianiu zależnie od potrzeb, można je lepiej wykorzystać. Chmura publiczna też prowadzi do oszczędności, wykorzystując specyfikę przetwarzania danych w systemach informatycznych (praca z przerwami, przy niewielkim procencie wykorzystywania dostępnych zasobów) oraz charakterystyczny sposób ich eksploatacji przez różne organizacje (inne pory dnia, tygodnia, r.). Usługi chmury publicznej są konkurencyjne z uwagi na ich skalowalność i elastyczność (Rogoziński 2013). W przypadku chmur prywatnych mogą pojawiać się problemy wydajnościowe ze względu na skupienie danych i aplikacji w niewielkich centrach.

W praktyce korzystne są tzw. chmury hybrydowe, łączące zalety obu rozwiązań – gdy dane o strategicznym znaczeniu pozostają na terenie organizacji, zaś pozostałe zasoby przenoszone są do chmury publicznej. Tak złożona struktura może stworzyć środowisko najlepiej dopasowane do potrzeb danej organizacji, jednak więcej uwagi wymaga zarządzanie siecią.

Do kompleksowego zarządzania infrastrukturą Data Center[9] proponuje się rozbudowane funkcjonalnie narzędzia, których przykładem może być System Center 2012 firmy Microsoft (*Przegląd* 2012). Istotną jego cechą jest pełne wsparcie nie tylko dla środowisk fizycznych, ale również dla rozwiązań wirtualnych. Wielomodułowy pakiet umożliwia, m.in. monitorowanie usług uruchamianych w tradycyjnym Data Center, w chmurze prywatnej i publicznej (moduł Operation Manager), zarządzanie pojedynczymi maszynami wirtualnymi oraz całą prywatną chmurą uruchamianą na kilku różnych wirtualizatorach (narzędzie Virtual Machine Manager) czy samodzielną szybką budowę, konfigurację, wdrożenie oraz zarządzanie usługami (moduł App Controler, obsługuje aplikacje wdrażane w chmurze prywatnej i publicznej). Ponadto narzędzie dostarcza mechanizm do tworzenia kopii systemów klienckich oraz Windows Server, dzięki czemu można chronić systemy instalowane zarówno na maszynach fizycznych, jak i wirtualne (Data Protection Manager). Ułatwia też wdrożenie i monitorowanie systemu ochrony antywirusowej (moduł Endpoint Protection). System Center 2012 znacząco zwiększa bezpieczeństwo zwirtualizowanej infrastruktury wprowadzając warstwowe podejście do planowania ochrony systemów, dzięki któremu można zagwarantować (chip.pl 2012):

- ochronę danych,
- nadzór nad wydajnością, dostępnością i bezpieczeństwem aplikacji,
- standaryzację konfiguracji zabezpieczeń,
- spójny model ochrony komunikacji sieciowej (między środowiskiem wirtualnym a użytkownikiem końcowym).

System Center działa też z wirtualizacją VMware i Citrixa (oprócz Hyper-V).

[9] Specjalistyczne centrum przetwarzania danych charakteryzujące się scentralizowanym zarządzaniem zasobami; dynamiczne centrum danych (*Dynamic Data Center*) cechują zautomatyzowane systemy operacyjne i elastyczne tworzenie topologii sieciowej.

4. Wirtualizacja a bezpieczeństwo

Platformy wirtualizacji tworząc odmienne i bardziej dynamiczne powiązania między zasobami informatycznymi w sposób istotny wpływają na bezpieczeństwo sieciowe. Nietypowość problemu bezpieczeństwa środowiska wirtualnego wynika, m.in. z możliwości modyfikacji maszyn wirtualnych także po ich wyłączeniu (stanowią pliki lub bloki na współdzielonych dyskach). Wymusza to sprawdzanie stanu maszyn przed każdym ich uruchomieniem. Środowisko wirtualne wiąże się z przenoszeniem maszyn między fizycznymi serwerami, często także między różnie zlokalizowanymi centrami przetwarzania danych, co może oznaczać zmianę praktyk dotyczących bezpieczeństwa. Problemy mogą też być powodowane łatwością i szybkością tworzenia kolejnych maszyn wirtualnych oraz wiążącą się z tym bardzo ograniczoną implementacją zasady segregacji obowiązków.

Dostrzega się także problem zagrożeń wynikający z wprowadzenia kolejnej warstwy oprogramowania, która może stwarzać dodatkowe luki w systemie zabezpieczeń, jednak zdaniem specjalistów, bezpieczeństwo rozwiązań wirtualnych to nie tylko ochrona na poziomie oprogramowania, ale także (a nawet w większym stopniu) sprzętu (Królikowski 2012).

Na poziom ryzyka wpływa również samo miejsce wirtualizacji oraz rodzaj przenoszonych w jej strefę zasobów. Nie powinno się na tej samej platformie uruchamiać systemów i aplikacji o różnych wymaganiach w zakresie bezpieczeństwa. Zagrożenia dla środowisk wirtualnych dotyczą też przestrzeni dyskowej i ruchu sieciowego – w obrębie platformy wirtualnej oraz pomiędzy maszynami. Problemem są technologie migracji zasobów z jednej platformy na inną, bowiem podczas przenoszenia VM istnieje możliwość podsłuchu. Najbardziej newralgicznym elementem jest hipernadzorca. Jego atrakcyjność, jako celu ataków, wynika z faktu, iż kontroluje wszystkie realizowane usługi i procesy na maszynach wirtualnych (Królikowski 2012).

Część platform wirtualnych jest zagrożonych atakiem VM Escape, ponieważ istnieje podatność w procesorach Intela, wynikająca ze sposobu implementacji instrukcji SYSRET (problem dotyczy platform, które ją wykorzystują). W innych (ESX) wykryto podatności, z których część umożliwiała eskalację uprawnień (Królikowski 2012).

Dostęp do platformy wirtualnej powinien być kontrolowany (najlepiej przez mechanizmy silnego uwierzytelniania), a dla ochrony systemu można użyć typowych rozwiązań do ochrony serwerów, zapory sieciowej, systemu detekcji intruzów oraz korzystać z połączeń VPN. Standardowe zabezpieczenia nie są tu jednak w pełni skuteczne, na przykład nie zapewnią kontroli ruchu sieciowego pomiędzy maszynami wirtualnymi w ramach hipernadzorcy. Dla zwiększenia bezpieczeństwa można też stosować specjalizowane narzędzia spoza platformy wirtualnej (służące na przykład do wzmocnienia kontroli uprawnień).

Wskazane jest jednak stosowanie narzędzi wykorzystujących mechanizmy bezpieczeństwa oferowane przez dostawców platform wirtualizacyjnych, takich jak VMware, który dostarcza zestaw trzech API VMsafe, do kontroli:

- dostępu do pamięci i stanów procesora (vCompute),
- przepływu danych między wirtualną kartą sieciową i wirtualnym przełącznikiem (vNetwork Appliance),
- wirtualnej przestrzeni dyskowej (VDDK).

VMsafe może być zastosowane nie tylko do ochrony punktów końcowych (przykładem rozwiązanie klasy Endpoint Security firmy Trend Micro), ale też w mechanizmach zapory sieciowej (na przykład firewall Virtual Gateway firmy Juniper). Innym oprogramowaniem przeznaczonym dla technologii wirtualnych jest vShield, które wprowadza dodatkowe mechanizmy ochronne, segmentację i tworzenie stref bezpieczeństwa. Właśnie aplikacje przeznaczone dla rozwiązań wirtualnych, takie jak oprogramowanie antywirusowe MOVE (*Management for Optimized Virtual Environments*) firmy McAfee obsługujące VMware vShield oraz HyTrust Appliance – m.in. wspierające kontrolę uwierzytelniania i wiązania użytkownika z kontami platformy wirtualnej, mogą zapewnić wysoki poziom ochrony. Oprogramowanie ochronne dla platformy VMware stworzyła też firma Kaspersky Lab, jednak na rynku nie ma wielu tego typu produktów.

Dla zwiększenia bezpieczeństwa można też wprowadzić szyfrowanie danych pomiędzy maszyną wirtualną a hipernadzorcą, czego przykład stanowi rozwiązanie zaproponowane przez firmę HighCloud Security (Królikowski 2012).

Przeniesienie infrastruktury do chmury wiąże się z utratą widoczności i możliwości zarządzania (wiele rozwiązań tego nie zapewnia). Z powodu wątpliwości dotyczących bezpieczeństwa, zamiast korzystania z chmury publicznej (wymagane wszystkie zabezpieczenia do ochrony sieci, bo dane pochodzą z różnych źródeł i trafiają do różnych odbiorców), proponuje się budowanie chmur prywatnych, które wykorzystują istniejącą infrastrukturę Data Center firm. Wirtualizacja stanowiąca podstawę dla chmury prywatnej wymaga od administratorów dużych umiejętności w zakresie nadzorowania bezpieczeństwa systemu (standardowe mechanizmy ochronne nie wystarczają). Ryzyko mogą zminimalizować częste aktualizacje systemu zabezpieczeń, na bieżąco usuwające wykrywane podatności na ataki.

Podsumowanie

Wirtualizacja wydaje się jedną z najbardziej perspektywicznych innowacji technologicznych w dziedzinie informatyki. Firmy dla potrzeb poszerzania i rozwijania oferty usług muszą zwiększać moc obliczeniową użytkowanych systemów informatycznych. Rozwiązanie niosą technologie wirtualizacji prowadząc do oszczędności finansowych organizacji, a także ograniczenia zużycia energii elektrycznej – stąd przewidywania dalszego wzrostu ich popularności.

Ochrona danych i usług w środowiskach wirtualnych stanowi zadanie priorytetowe, dlatego wymagane jest stosowanie specjalistycznych narzędzi w postaci zintegrowanych mechanizmów zapewniających kompleksową ochronę całej wielowarstwowej infrastruktury. Konieczne jest też zaangażowanie zespołu ds. bezpieczeństwa w proces wdrażania wirtualizacji już w fazie projektowania zamierzenia oraz właściwe przeszkolenie personelu obsługującego.

Stosowanie rozwiązań wirtualnych infrastruktury informatycznej wymaga kompromisu między potencjalnymi korzyściami wynikającymi z ich wdrożenia a pożądanym poziomem bezpieczeństwa. Przed podjęciem decyzji o wirtualizacji należy też przeanalizować strukturę i infrastrukturę organizacji (w czym pomagają odpowiednie narzędzia), a następnie rozważyć stosunek korzyści do kosztów, gdyż oprogramowanie do wirtualizacji, jak dotąd, nie jest tanie.

Literatura

Adelberger S. (2012), *Wirtualizacja a kwestie bezpieczeństwa danych*. virtual-it.pl/artykuly/3151-wirtualizacja-a-kwestie-bezpieczenstwa-danych.html (dostęp 2013).

Bittman T.J., Weiss G.J., Margevicius M.A., Dawson P. (2012), *Magic Quadrant for x86 Server Virtualization Infrastructure*, Raport, Gartner 2012. virtual-it.pl/3283-magic-quadrant-for-x86-server-virtualization-infrastructure-2012.html (dostęp 2013).

chip.pl/news/oprogramowanie/wirtualizacja/2012/05/jak-stworzyc-bezpieczne-srodowisko-wirtualne (2012).

Citrix Report – *Virtualisation to dominate enterprise IT savings by 2014* (2010), citrix.com/news/market-research/feb-2010/virtualisation-to-dominate-enterprise-it-savings-by-2014.html (dostęp 2013).

Królikowski P. (2012), *Realne zagrożenia wirtualizacji*. www.computerworld.pl/artykuly/384031/Realne.zagrożenia.wirtualizacji.html (dostęp 2013).

Porowski D. (2011), *Co to jest wirtualizacja*, Microsoft. http://technet.microsoft.com/pl-pl/library/co-to-jest-wirtualizacja.aspx (2014).

Przegląd możliwości nowego Microsoft System Center 2012. Kompleksowe zarządzanie infrastrukturą datacenter, chip.pl/news/oprogramowanie/programy-biurowe/2012/05/kompleksowe-zarzadzanie-infrastruktura-datacenter (2012).

riverbed.com/about/news-articles/press-releases/riverbed-and-vmware-preview-lan-performance-for-distributed-vmware-view-environments.html (2012).

Rogoziński D. (2013), *Publiczna, prywatna czy hybrydowa – która chmura najlepsza?*, www.virtual-it.pl/artykuly/3881-publiczna-prywatna-czy-hybrydowa-ktora-chmura-najlepsza.html.

Serafin M. (2011), *Wirtualizacja w praktyce*, Helion, Gliwice.

Wojtczak S.W. (2008), *Wirtualizacja systemów operacyjnych*, Uniwersytet Łódzki, Łódź, strony.toya.net.pl/~vermaden/tmp/thesis.pdf (dostęp 2014).

THE COMPETITIVENES OF VIRTUAL SOLUTIONS FOR IT INFRASTRUCTURE

Summary

In order to be able to deploy new services and develop existing services, companies need to constantly increase their computing power capabilities. Virtual infrastructure solutions lead to optimal use of resources and energy savings. Because of the many advantages and a wide range of applications they are increasingly willingly implemented, especially by small and medium-sized companies. An interesting offer is also cloud computing. Virtualization tools are being systematically developed, however, due to the growing problem of network threats and because of the specific nature of virtualization technologies, more attention should be focused on the issues of security of these environments.

Keywords: virtual machines, cloud computing, security of virtual environment

Translated by Zygmunt Mazur