INFORMATYKA EKONOMICZNA BUSINESS INFORMATICS 3(41) • 2016

ISSN 1507-3858
e-ISSN 2450-0003

Artur Rot
Uniwersytet Ekonomiczny we Wrocławiu
e-mail: artur.rot@ue.wroc.pl

WYBRANE PODATNOŚCI I ZAGROŻENIA BEZPIECZEŃSTWA ŚRODOWISKA WIRTUALNEGO W ORGANIZACJI

SELECTED SECURITY VULNERABILITIES AND THREATS IN THE VIRTUAL ENVIRONMENT IN ORGANIZATIONS

DOI: 10.15611/ie.2016.3.06
JEL Classification: M15, O33

Streszczenie: Wdrożenie w organizacji technologii wirtualnych pozwala uzyskać wiele korzyści, wśród których najważniejsze to lepsze wykorzystanie zasobów informatycznych oraz wyższa ich wydajność, skrócenie reakcji organizacji na potrzeby biznesowe przez dynamiczną optymalizację środowisk oprogramowania, ograniczenie kosztów przyszłej rozbudowy infrastruktury IT, niższe nakłady operacyjne oraz wyższy stopień bezawaryjności i zapewnienie ciągłości działania systemów informatycznych. Jednakże potencjalne zalety tych rozwiązań nie mogą przysłaniać niezwykle istotnej kwestii, jaką jest zapewnienie bezpieczeństwa systemom pracującym w środowisku wirtualnym. Ze względu na dużą liczbę zagrożeń i podatności wymaga ono stosowania specjalistycznych narzędzi, a także odpowiednich umiejętności od administratorów systemów IT. Artykuł prezentuje zalety i możliwości tej formy organizacji środowiska informatycznego, ale przede wszystkim wyszczególnia wiele podatności i zagrożeń, na jakie jest ono narażone.

Słowa kluczowe: wirtualizacja, maszyny wirtualne, bezpieczeństwo środowiska wirtualnego, zagrożenia, podatności.

Summary: The implementation of virtual machines allows an organization to gain a number of advantages, among which the most important are better use of IT resources and their productivity, shortening the reaction of an enterprise to business needs by dynamic optimization of the software environment, costs reduction of future expansion of the IT infrastructure, lower capital and operating expenditures and a higher degree of reliability and business continuity of IT systems. However, the potential benefits of these solutions cannot obscure a very important issue, which is the security of systems running in a virtual environment. Due to a number of threats and vulnerabilities it requires the implementation of special tools as well as relevant administrative skills. The aim of this article is to identify opportunities and savings of this form of IT organization, but first of all, to present the vulnerabilities and threats of the virtual environment.

Keywords: virtualization, virtual machines, virtual environment security, threats, vulnerabilities.

1. Wstęp

Turbulentne otoczenie powoduje, iż współczesne organizacje wciąż poszukują nowych rozwiązań w zakresie organizacji i zarządzania, które są nierozerwalnie związane z systemami informatycznymi odgrywającymi istotną rolę w procesie podejmowania decyzji. Środowisko informatyczne zaczyna mieć kluczowe znaczenie dla dzisiejszych organizacji, które oczekują większej elastyczności i szybszego działania systemów informatycznych, a także wyższej wydajności i kontroli nad kosztami. Wdrażanie nowych usług z wykorzystaniem środowisk wirtualnych oraz migracja już funkcjonujących do tego typu rozwiązań będą z pewnością w najbliższych latach zyskiwać na popularności. Dlatego też wirtualizacja wydaje się aktualnie jedną z najbardziej perspektywicznych innowacji technologicznych w obszarze informatyki. Daje ona wiele korzyści, gdyż rozwiązania wirtualne prowadzą do optymalnego wykorzystania istniejących zasobów, a także przyczyniają się do znacznych oszczędności, dlatego też są one cały czas rozwijane. Jednakże ze względu na coraz większą liczbę zagrożeń szczególną uwagę należy zwrócić na kwestię bezpieczeństwa, która stanowi jeden z najważniejszych aspektów wirtualizacji i nad którą trwają aktualnie intensywne prace. Celem artykułu jest wskazanie możliwości i oszczędności, jakie niesie za sobą środowisko wirtualne, ale przede wszystkim przedstawienie podatności i zagrożeń jakim ono podlega. W artykule wskazano też najważniejsze mechanizmy, jakie powinny być stosowane, aby zapewnić odpowiedni poziom bezpieczeństwa omawianym rozwiązaniom. Zawarte w tekście rozważania wynikają zarówno z badań literaturowych, jak i doświadczeń autora, będących efektem kierowania projektem wdrożenia wirtualnego środowiska na Uniwersytecie Ekonomicznym we Wrocławiu. W przygotowanej przez kierownictwo uczelni Strategii rozwoju na lata 2010–2020 jednym z postulatów wskazującym kierunki rozwoju jest poprawa sprawności funkcjonalnej uczelni i wszystkich jej jednostek organizacyjnych przez pełną integrację w oparciu o zaawansowane systemy informatyczne oraz rozwój sieci informatycznej i zwiększenie jej bezpieczeństwa celem lepszego dostosowania do potrzeb dydaktyki, badań i zarządzania. Odpowiedzią na te wyzwania było stworzenie wirtualnego środowiska, które nie tylko obsługuje aktualnie istniejące usługi i systemy na uczelni, ale także pozwoliło na zastosowanie w badaniach naukowych i procesie dydaktycznym najnowszych rozwiązań informatycznych.

2. Istota wirtualizacji infrastruktury informatycznej

Środowisko informatyczne ma kluczowe znaczenie dla większości współczesnych organizacji. Jednakże infrastruktury informatyczne stają się zbyt złożone i podatne na awarie, aby mogły dotrzymywać kroku tempu i dynamice rozwoju przedsiębiorstw i instytucji. Użytkownicy oczekują krótszych czasów reakcji, a kierownictwo − minimalizacji kosztów, przez co niezbędna jest m.in. lepsza strategia wykorzystania zasobów informatycznych [Szyjko 2012]. Aplikacje uruchamiane na współczesnych, wydajnych komputerach obciążają je często jedynie w niewielkim

stopniu (według różnych szacunków 10-25%). Niejednokrotnie podobnie sytuacja wygląda w przypadku serwerów: ich usługi również absorbują tylko część ich potencjału. Wirtualizacja rozwiązuje ten mało efektywny model, umożliwiając obsługę wielu serwerów wirtualnych na jednym serwerze fizycznym, co znacznie zwiększa wykorzystanie zasobów istniejącej infrastruktury serwerowej bez utraty funkcjonalności, a co najważniejsze – również jej wydajności.

Samą wirtualizację można interpretować jako „osiągnięcie logicznego zasobu przez abstrakcję zasobów fizycznych" [Porowski 2011]. Podstawą wirtualizacji środowiska informatycznego jest wyodrębnianie specyficznych cech i zadań elementów infrastruktury technologii informacyjnej (IT) i uruchamianie ich w sposób abstrakcyjny, z wykorzystaniem obcych rozwiązań programowych, sieciowych i sprzętowych, z zachowaniem pełnej funkcjonalności [Rule, Dittner 2007]. Wirtualizacja w takim razie polega na izolowaniu jednego zasobu obliczeniowego od pozostałych, co prowadzi do uzyskania korzyści w postaci zwiększenia elastyczności systemu oraz ułatwienia zarządzania zmianami. Natomiast maszyna wirtualna (*Virtual Machine* − VM) to środowisko wirtualne dla działania programów, które ma kontrolę nad wirtualizowanymi zasobami. Wirtualizacja pozwala na integrację wielu niezależnie działających systemów informatycznych i na uruchomienie już zintegrowanego systemu na kilku fizycznych maszynach.

Jednakże wirtualizacja nie stanowi nowego podejścia do zarządzania infrastrukturą informatyczną, ponieważ technologia tworzenia środowiska wirtualnego została zaproponowana już kilkadziesiąt lat temu. Pierwsze próby związane z wirtualizacją pochodzą z lat 60., kiedy problemem tym zajęła się firma IBM. W roku 1964 rozpoczęto pracę nad systemem CP-40 dla komputerów mainframe System/360, który miał zapewnić równoczesną pracę maszyn wirtualnych. Celem tych działań było umożliwienie wykorzystania tych komputerów do wykonywania kilku zadań jednocześnie. Stworzony przez tę firmę system operacyjny VM/370 oferował praktycznie niemal wszystkie możliwości, jakie dostępne są we współczesnych programach maszyn wirtualnych [Arce 2007]. Przez wiele lat koncepcja wirtualizacji z powodzeniem wykorzystywana była głównie w zastosowaniach wojskowych i przemysłowych, na wspomnianych komputerach typu *mainframe*. Obecnie wirtualizacja weszła do powszechnego użytku i jest aktualnie uważana za jeden z najważniejszych kierunków rozwoju informatyki. Wzrost mocy obliczeniowej komputerów osobistych pozwala na wydajne wirtualizowanie nawet kilku systemów operacyjnych jednocześnie [Kaczmarek Wróbel 2011]. Stale rośnie liczba wdrażanych projektów wirtualizacji serwerów, a to głównie dzięki korzyściom, jakie daje ta technologia. Ze względu na nie wirtualizacja jest obecnie technologią, która bardzo mocno zyskuje na znaczeniu w centrach danych. Najważniejsze korzyści, do których zaliczyć można m.in. oszczędności uzyskane z ograniczenia zakupów, serwisowania i zasilania nowych serwerów fizycznych, będą przedmiotem rozważań w dalszej części niniejszego artykułu.

W latach 80. amerykańscy naukowcy Gerald J. Popek i Robert P. Goldberg [Popek, Goldberg 1974] zdefiniowali podstawowe kryteria właściwego funkcjonowania

maszyny wirtualnej (kryteria jakości wirtualizacji) [Roszkowski 2011], która powinna spełniać trzy podstawowe warunki:

- odpowiedniość (*equivalence*) – aplikacja uruchomiona na wirtualnej maszynie musi funkcjonować identycznie jak na rzeczywistym komputerze,
- kontrola zasobów (*resource control*) – zwirtualizowane zasoby powinny być w pełni kontrolowane przez wirtualną maszynę,
- wydajność (*efficiency*) – większość instrukcji powinna być wykonywana bez pośrednictwa maszyny wirtualnej.

Wirtualizacja pozwala na efektywne wykorzystanie istniejącego sprzętu informatycznego przez modyfikowanie cech wirtualizowanych zasobów zgodnie z potrzebami użytkowników [Mendyk-Krajewska, Mazur, Mazur 2014]. Jest ona bardzo szerokim pojęciem i może dotyczyć [IBM 2007]:

- Sieci komputerowych – wirtualizacja sieci zwiększa elastyczność wykorzystania zasobów, poprawia wykorzystanie pojemności oraz umożliwia segmentację sieci, a co za tym idzie − podnosi znacznie poziom bezpieczeństwa sieci [Przybylak 2010].
- Magazynów danych (pamięci masowych) – wirtualizacja pamięci masowych pozwala agregować dane przechowywane w urządzeniach pamięci masowych i umieszczać je w puli zasobów, do której można uzyskać szybko dostęp i którą można łatwo zarządzać z jednego, centralnego miejsca. Dzięki temu użytkownik nie widzi całej złożoności pamięci masowych, a jedynie udostępniony mu jest logiczny obraz danych, odseparowany od skomplikowanej struktury urządzeń fizycznych. Zatem wirtualizacja pamięci masowych daje możliwość, aby wiele macierzy dyskowych było widocznych jako jedno wirtualne urządzenie, do którego podłączają się użytkownicy.
- Serwerów – ten najbardziej popularny obszar stosowania technik wirtualizacyjnych polega na wydzieleniu w obrębie jednego serwera fizycznego wielu mniejszych środowisk wirtualnych, co umożliwia optymalne rozdzielenie zasobów procesora, pamięci operacyjnej RAM i pamięci masowych między wiele działających jednocześnie procesów.
- Systemów operacyjnych – daje to możliwość uruchomiania systemu operacyjnego wewnątrz już istniejącego. System zainstalowany na komputerze fizycznym zwany jest gospodarzem (*host*), zaś te uruchomione na maszynach wirtualnych to goście (*guests*). Dzięki temu otrzymujemy systemy pracujące jednocześnie na tej samej fizycznej maszynie, która rozdziela zasoby sprzętowe (pamięć RAM, pamięć masowa, procesor) komputerom typu „gość" według potrzeb.
- Aplikacji – polega na izolacji od siebie różnych aplikacji, co rozwiązuje problem ich zgodności, umożliwiając im działanie razem. Dzięki wirtualizacji aplikacje zmieniają się w centralnie zarządzane usługi, które nie powodują konfliktów z innymi programami. Znacznie usprawnia to również proces testowania oprogramowania.

- Stacji roboczych – wirtualizacja komputerów roboczych (desktopów) jest rozwinięciem idei wirtualizacji aplikacji. Obejmuje jednak więcej zasobów komputera. W tym przypadku wirtualizacji podlegają bowiem warstwy: systemu operacyjnego, aplikacji oraz indywidualnych ustawień (profili) użytkownika [Turek 2011].

Obserwując szeroki zakres wirtualizacji, pokusić się można o tezę, iż stanowi ona przyszłość informatyki, chociaż są, oczywiście, pewne dziedziny, w których nie ma ona jeszcze tak dużego znaczenia czy też praktycznego zastosowania. Jednakże w przyszłości będzie ona z pewnością stosowana na jeszcze większą skalę niż aktualnie.

3. Korzyści wynikające z wirtualizacji środowiska informatycznego

Wirtualizacja szybko została zaadaptowana przez organizacje, gdyż, jak wspomniano, oferuje wiele korzyści, wśród których jedną z najistotniejszych jest obniżenie nakładów inwestycyjnych oraz kosztów operacyjnych. Efekty te uzyskiwane są dzięki konsolidacji serwerów, a więc optymalizacji stopnia zużycia istniejącej infrastruktury informatycznej w celu redukcji kosztów ponoszonych przez przedsiębiorstwa i instytucje na zapewnienie wysokiej dostępności. Dzięki niej można uprościć istniejące środowisko IT, tworząc przy tym dynamiczniejsze i bardziej elastyczne centrum przetwarzania danych. Dla części organizacji staje się ona również sposobem na oszczędność miejsca w serwerowniach.

Kolejne ważne korzyści to możliwość uruchomienia na jednym serwerze kilku maszyn wirtualnych, elastyczność konfiguracji zasobów, scentralizowane zarządzanie, mniejsze zużycie energii przez komputery oraz systemy chłodzenia (dlatego też czasami wirtualizację nazywa się „zieloną techniką"). Jak widać, wirtualizacja środowiska informatycznego ma dużo zalet, które w przypadku organizacji mogą się z pewnością przełożyć na wymierne korzyści, a także mieć wpływ na osiągnięcie przez nią przewagi konkurencyjnej. Wyliczając liczne zalety wirtualizacji, można wymienić następujące korzyści z niej płynące [Roszkowski 2011; Czajkowski 2011; Scheffy 2007]:

- Konsolidacja serwerów, a dzięki temu optymalizacja stopnia zużycia posiadanego sprzętu komputerowego i lepsze wykorzystanie zasobów obliczeniowych (*computing assets*) przez zwiększenie utylizacji serwerów wirtualnych na serwerach fizycznych, dzięki czemu lepiej wykorzystywane są zasoby obliczeniowe tych drugich.
- Poprawienie reakcji na potrzeby biznesowe przez dynamiczną optymalizację środowisk oprogramowania – szybkie dostarczanie odpowiednich zasobów IT dla określonych procesów biznesowych, co nie wymaga pozyskania nowego sprzętu informatycznego i daleko idących zmian w istniejącej infrastrukturze IT. Dzięki takiej elastyczności odpowiednie planowane zmiany w działalności

biznesowej mogą być z powodzeniem szybko wprowadzane przez organizację, co daje również większą możliwość wykorzystania nowych szans biznesowych.
- Redukcja całkowitych kosztów aktywów w przedsiębiorstwie w ramach modelu TCO (*Total Cost of Ownership*) – TCO to całkowity koszt pozyskania, instalowania, użytkowania, utrzymywania i pozbycia się aktywów w organizacji w określonym czasie. Służy on do oceny bieżących i prognozowanych wydatków lub kosztów infrastruktury IT. Jego obniżenie następuje przez zwiększenie wykorzystania sprzętu i konsolidację serwerów. Redukcja kosztów jest prowadzona na trzech poziomach jednocześnie; są nimi: ludzie, technologie i procesy.
- Ograniczenie kosztów przyszłej rozbudowy infrastruktury IT – potrzeba rozbudowy środowiska IT o nowe usługi, które muszą być świadczone przez serwery, związana jest jedynie z koniecznością stworzenia nowej maszyny wirtualnej wraz z serwerem. W tej sytuacji pojawi się koszt licencji na użytkowanie nowego serwera wirtualnego. Minimalizacji ulegają koszty związane z fizycznym miejscem dla nowego systemu operacyjnego.
- Niższe nakłady inwestycyjne CAPEX (*capital expenditures*) – oszczędności zyskiwane są przede wszystkim dzięki mniejszej liczbie fizycznych serwerów, interfejsów, okablowania sieciowego oraz różnych urządzeń sieciowych.
- Niższe koszty operacyjne OPEX (*operating expenditures*) – oszczędności te wynikają m.in. ze zmniejszenia zapotrzebowania na energię elektryczną, z ograniczenia kosztów serwisu oraz lepszego wykorzystania miejsca w serwerowni itp.
- Bezawaryjność i ciągłość działania systemów informatycznych – systemy informatyczne mogą pracować w sposób ciągły, bez zakłóceń dzięki technologiom wspomagającym pracę maszyn wirtualnych. Bezawaryjność tę uzyskuje się m.in. przez podział obciążeń pracą. Podział ten zapobiega sytuacjom, gdy niepoprawne działanie jednej aplikacji ma negatywny wpływ na wydajność innych systemów lub powoduje utratę ciągłości działania systemu (możliwe jest używanie niestabilnych aplikacji w odizolowanym i bezpiecznym środowisku).
- Wzrost bezpieczeństwa i niezawodności infrastruktury dzięki właściwościom wysokiej dostępności (*high availability*) platformy wirtualizacji. Serwery wirtualne mogą być przenoszone w czasie pracy między maszynami fizycznymi czy to na skutek awarii sprzętu, czy podczas prac rekonfiguracyjnych.
- Możliwość budowy rozwiązań odtwarzania awaryjnego (*disaster recovery*), dzięki możliwości automatycznego uruchomienia serwera wirtualnego w ośrodku zapasowym, po awarii podstawowego centrum przetwarzania danych.
- Możliwość uruchomienia kilku różnych systemów operacyjnych w tym samym czasie, co daje potencjał do wykorzystania ich zalet, gdyż nic nie stoi na przeszkodzie, aby maszyna pod kontrolą np. systemu operacyjnego Linux uruchamiała na maszynie wirtualnej system operacyjny Windows i oprogramowanie działające w środowisku Linux [Cranitch, Rees 2009].
- Możliwość uruchomienia niekompatybilnego oprogramowania na nowym i wydajniejszym sprzęcie komputerowym, czyli zdolność obsługi starszych wersji

programów oraz aplikacji biznesowych, często niewspółpracujących z aktualnie eksploatowanymi systemami operacyjnymi serwerów. Dzięki wirtualizacji aplikacji i udostępnianiu ich na żądanie skrócony zostaje również czas potrzebny do testowania kompatybilności oprogramowania.

- Scentralizowane zarządzanie infrastrukturą – systemy operacyjne zainstalowane na serwerach wirtualnych wymagają tworzenia kopii bezpieczeństwa, instalacji aktualizacji i poprawek do systemu operacyjnego lub zainstalowanego oprogramowania i podejmowania wielu innych czynności. Wszystkie operacje, które muszą być wykonywane na serwerach wirtualnych, są zlecane jednej centralnej konsoli zarządzającej i są przez nią nadzorowane.

Podsumowując, można stwierdzić, iż wirtualizacja zwiększa wykorzystanie serwerów przez konsolidację wielu usług na pojedynczej maszynie fizycznej. Pozwala na znaczne obniżenie wydatków inwestycyjnych i operacyjnych, jak i łatwiejsze oraz tańsze zarządzanie infrastrukturą informatyczną. Wirtualizacja serwerów przynosi również wzrost bezpieczeństwa i niezawodności infrastruktury przez zwiększenie dostępności oprogramowania i ciągłości biznesowej niezależnie od sprzętu i systemów operacyjnych, a także dzięki możliwości budowy rozwiązań typu *disaster recovery*. Pozwala także przedsiębiorstwom na szybkie zmiany i reagowanie na powstające potrzeby biznesowe przez dynamiczną optymalizację środowisk oprogramowania.

4. Zagrożenia bezpieczeństwa w środowisku wirtualnym

Jak wskazano, dzięki wirtualizacji organizacja może uzyskać wiele korzyści, jednakże wywołuje ona również pewne problemy i niesie wyzwania związane z kwestią bezpieczeństwa. Wiele osób zwraca uwagę na zalety omawianych rozwiązań, ale nie widzi ich złożoności. W związku z tym, iż wirtualne środowisko IT jest odmienne i ma inne właściwości niż klasyczne, wymaga również odmiennego podejścia do problematyki zabezpieczeń. Porównując potencjał zagrożeń fizycznych systemów i maszyn wirtualnych, można stwierdzić, iż poziom podatności na ataki jest podobny. Środowisko wirtualne stoi w obliczu podobnych zagrożeń, jednakże wirtualizacja wprowadza kolejną warstwę oprogramowania, która również narażona jest na liczne zagrożenia, a także jest podatna na działanie intruzów lub złośliwego oprogramowania. W związku z tym pojawiają się kolejne zagrożenia, które muszą być brane pod uwagę przez administratorów bezpieczeństwa. Ponadto konsekwencje nadużyć w wirtualnym środowisku mogą być dużo bardziej poważne niż w przypadku klasycznych rozwiązań, ponieważ platformy wirtualne na ogół dają możliwość dostępu do wielu różnych zasobów [Rot 2016]. Niezabezpieczone środowisko wirtualne może otworzyć drzwi do pozostałej części sieci, stąd też ataki na taką infrastrukturę mogą być atrakcyjnym celem cyberprzestępców. Wiele niebezpieczeństw związanych jest z hipernadzorcą (*hypervisor*), który jest programem nadzorującym funkcjonowanie maszyn wirtualnych, określanym jako monitor maszyn wirtualnych

(*Virtual Machine Monitor* − VMM). Złamanie zabezpieczeń hipernadzorcy pozwala przeprowadzić skuteczny atak (*hyperjacking*) i uzyskać dostęp do wszystkich wirtualnych maszyn działających na danym serwerze fizycznym [Janus 2008].

Jedną z największych korzyści wirtualizacji jest izolacja, czyli odseparowanie środowisk roboczych, która nieprawidłowo wdrożona, może generować poważne zagrożenia dla całego środowiska wirtualnego [Luo, Lin, Chen 2011]. Nieprawidłowe odseparowanie lub nieodpowiednia polityka kontroli dostępu może spowodować ataki między maszynami wirtualnymi. Jednym z najpoważniejszych zagrożeń są w tym przypadku ataki typu *VM Escape*, które stają się realne, jeśli izolacja między hostem a maszynami wirtualnymi jest zagrożona. Podczas tych ataków program uruchomiony na maszynie wirtualnej jest w stanie ominąć zabezpieczenia i uzyskać dostęp do hosta. Ponieważ urządzenie hosta jest źródłem bezpieczeństwa systemu wirtualnego, program, który uzyskuje dostęp do komputera hosta, również nabywa przywileje administratora [Indumathy 2015].

Istotnym wyzwaniem, któremu muszą sprostać administratorzy bezpieczeństwa środowiska wirtualnego, jest łatwość tworzenia nowych serwerów wirtualnych. Często powstają one z już istniejących obrazów w porę niezaktualizowanych i zawierających istotne luki, które mogą zostać wykorzystane przez złośliwe oprogramowanie lub intruzów, mogących przejąć kontrolę nad maszyną wirtualną. To z kolei daje duże możliwości przejęcia kontroli nad kolejnymi maszynami wirtualnymi wewnątrz całego środowiska [Pomorski 2009].

Kolejne zagrożenie wiąże się z podatnością na działanie szkodliwego oprogramowania. W środowisku wirtualnym oprogramowanie, również to szkodliwe, może działać tak samo jak w środowisku fizycznym. W związku z tym maszyny wirtualne są w podobnym stopniu podatne na ataki szkodliwego oprogramowania. Zagrożenia pochodzą od wirusów załączanych do poczty e-mail, trojanów, robaków, a także ze strony ataków phishingowych. Maszyny wirtualne są mniej podatne na zagrożenia, takie jak oprogramowanie szpiegujące (*spyware*) i oprogramowanie używane w przestępczości internetowej (*ransomware*), jednak systemy te wciąż mogą zostać zainfekowane innymi rodzajami szkodliwego oprogramowania [Kupczyk 2011].

Problemem są również technologie migracji zasobów wirtualnych z jednej platformy do drugiej (np. *vMotion*). Niestety, w trakcie przenoszenia maszyny można bez większych przeszkód podsłuchać ruch (otwarty tekst) i wyciągnąć informacje chronione znajdujące się akurat w danej chwili w pamięci operacyjnej RAM [Królikowski 2012]. W środowisku wirtualnym każdy gość współdzieli pewne zasoby, które mogą stać się celami ataku, a niezabezpieczone fizyczne węzły komunikacji mogą stać się platformą umożliwiającą przeprowadzenie podsłuchu danych (tzw. *sniffing*) [Carvalho 2009].

W architekturze maszyn wirtualnych goście i hosty współdzielą fizyczne zasoby, takie jak procesor, pamięć i zasoby sieciowe. Możliwe jest zatem przeprowadzenie ataku DoS (*Denial of Service*) przez jeden z systemów typu „gość" w stosunku do pozostałych, będących elementem całego systemu wirtualnego. Atak DoS w środo-

wisku wirtualnym może zostać zdefiniowany jako atak, w którym jedna z maszyn wirtualnych zajmuje wszystkie współdzielone zasoby systemu, uniemożliwiając innym uprawnionym maszynom korzystanie z nich. Odpowiedzią na taką sytuację może być wcześniejsze ustawienie limitów zasobów przydzielanych poszczególnym maszynom wirtualnym, co oferowane jest jako jedna z możliwości współczesnych technologii wirtualizacyjnych [Reuben 2007].

Jak wspomniano w artykule, maszyna hosta zarządza systemami wirtualnymi i innymi komputerami typu „gość", a środowisko wirtualne ułatwia takie zarządzanie. Komputery typu „host" mają w tym celu konsolę zarządzającą, która również może stać się celem ataku, a następnie za jej pośrednictwem intruz może przejąć kontrolę nad środowiskiem wirtualnym [Sobati 2013]. Różne technologie wirtualizacyjne dają komputerom hostom odmienne możliwości kontroli maszyn wirtualnych pracujących w danym środowisku. Host może mieć wiele różnych uprawnień, np. [Kirch 2007]:

- uruchamianie, zatrzymywanie i restart maszyn wirtualnych,
- monitorowanie i modyfikacja zasobów dostępnych dla maszyn wirtualnych,
- monitorowanie aplikacji uruchomionych przez maszyny wirtualne,
- przeglądanie, kopiowanie i modyfikowanie danych zgromadzonych na dyskach wirtualnych przypisanych do maszyn wirtualnych.

Ze względu na wspomniane uwarunkowania konieczne jest szczególne zabezpieczenie maszyn typu „host" w sposób dokładniejszy niż poszczególnych maszyn wirtualnych.

Omówione rodzaje ryzyka to tylko część najważniejszych zagrożeń i podatności, z jakimi można mieć do czynienia w środowisku wirtualnym. Odpowiedzią na nie jest konieczność stosowania wielopoziomowej ochrony takiego środowiska. Przede wszystkim wskazane jest stosowanie narzędzi wykorzystujących mechanizmy bezpieczeństwa oferowane przez dostawców platform wirtualizacyjnych [Mendyk-Krajewska, Mazur, Mazur 2014]. Dostęp do platformy wirtualnej powinien być także kontrolowany z wykorzystaniem mechanizmów silnego uwierzytelnienia. System bezpieczeństwa powinien stosować również rozwiązania typowe dla ochrony sieci, takie jak np.:

- tworzenie wirtualnych sieci lokalnych VPN, będących tunelami, przez które płynie ruch w ramach sieci w taki sposób, że węzły tej sieci są przezroczyste dla przesyłanych w ten sposób pakietów (można opcjonalnie szyfrować przesyłane dane w celu zapewnienia wyższego poziomu bezpieczeństwa),
- wdrażanie sprawdzonych, bezpiecznych i wydajnych urządzeń i systemów sieciowych, takich jak ściany ogniowe czyli firewalle (służące do zabezpieczania sieci i systemów przed intruzami), filtry pakietów danych (selektywne przepuszczanie lub blokowanie pakietów przechodzących przez interfejs sieciowy), systemy autentykacji (systemy weryfikujące zadeklarowaną tożsamość podmiotu biorącego udział w procesie komunikacji itp.),
- instalacja odpowiedniego oprogramowania antywirusowego,

- szyfrowanie danych – w celu zwiększenia bezpieczeństwa można też wprowadzić szyfrowanie danych między maszyną wirtualną a hipernadzorcą.

Ryzyko związane ze stosowaniem wirtualizacji może być także znacznie zredukowane dzięki częstym aktualizacjom systemu zabezpieczeń oraz bieżącym eliminacjom występujących podatności na zagrożenia. Ponadto środowisko wirtualne w organizacji wymaga od administratorów dużych umiejętności w nadzorowaniu systemu bezpieczeństwa, dlatego też istotne jest również przestrzeganie dyscypliny procedur administracyjnych.

Standardowe mechanizmy nie są jednakże w pełni skuteczne w wirtualnym środowisku, dlatego też w celu zwiększenia poziomu bezpieczeństwa powinny stosowane być specjalizowane narzędzia spoza platformy wirtualnej, służące np. do wzmocnienia kontroli uprawnień [Mendyk-Krajewska, Mazur, Mazur 2014].

5. Zakończenie

Znana organizacja badawcza Garner, zajmująca się m.in. analizą rynku IT, corocznie publikuje listę dziesięciu najważniejszych dla organizacji i użytkowników technologii informacyjnych, wśród których od kilku lat stale pojawia się wirtualizacja zasobów IT. Technologia ta ma aktualnie coraz więcej różnorodnych zastosowań. Swoje rozwiązania odnajduje nie tylko w stosunku do serwerów, ale także stacji roboczych, systemów operacyjnych, aplikacji, pamięci i sieci komputerowych. Przynosi ona wymierne korzyści w zakresie organizacji IT, dlatego też wirtualizacja szybko wchodzi do powszechnego użytku. Wprowadza ona dodatkowe techniki, komponenty i oferuje możliwości, które jednocześnie stwarzają nowe wyzwania i narażone są na wiele zagrożeń związanych z bezpieczeństwem, w związku z tym zabezpieczenia stosowane w odniesieniu do środowisk wirtualnych różnią się od zabezpieczeń systemów klasycznych. Ponadto w centrum danych serwer fizyczny może pomieścić dziesiątki lub setki maszyn wirtualnych, co powoduje, iż należy poświęcać szczególną uwagę kwestiom bezpieczeństwa, projektując wirtualne środowisko, a następnie administrując nim.

Literatura

Arce I., 2007, *Ghost in the virtual machine*, IEEE Security & Privacy, vol. 5, no. 4, s. 68-71.

Carvalho J.C., 2009, *Security Challenges with Virtualization*, master's thesis, Department of Informatics, Lisboa University.

Cranitch G., Rees M., 2009, *Virtualisation: A case study in database administration laboratory work*, Proceedings of ASCILITE 2009: Same places, different spaces, Auckland, http://www.ascilite.org.au/conferences/auckland09/procs/cranitch.pdf (16.12.2016).

Czajkowski A., 2011, *Wirtualizacja jako narzędzie wspomagające nauczanie na poziomie studiów wyższych na kierunkach informatycznych*, [w:] *Projektowanie w komputerowym wspomaganiu procesu dydaktycznego*, Baron-Polańczyk E. (red.), Oficyna Wydawnicza Uniwersytetu Zielonogórskiego, Zielona Góra.

IBM, 2007, *Virtualization in Education*, Global Education White Paper, http://www-07.ibm.com/solutions/in/education/download/Virtualization%20in%20Education.pdf (7.01.2017).

Indumathy M., 2015, *Survey on virtualization vulnerabilities,* International Journal of Science, Technology and Management, vol. 04, special issue no. 01, March.

Janus R., 2008, *Wirtualizacja a bezpieczeństwo*, IT Focus, 27.12.2008, http://itfocus.pl/dzial-it/sieci/wirtualizacja-a-bezpieczenstwo/ (18.01.2017).

Kaczmarek J., Wróbel M., 2011, *Możliwości stosowania wirtualizacji w systemach komputerowych*, Zeszyty Naukowe Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej nr 30/2011, XXI Seminarium „Zastosowanie Komputerów w Nauce i Technice 2011", Oddział Gdański PTETiS, Wydawnictwo Politechniki Gdańskiej, Gdańsk.

Kirch J., 2007, *Virtual Machine Security Guidelines*, The Center for Internet Security, September 2007, http://www.cisecurity.org/tools2/vm/CIS_VM_Benchmark_v1.0.pdf (11.01.2017).

Królikowski P., 2012, *Realne zagrożenia wirtualizacji*, Computerworld, 29.10.2012, http://www.computerworld.pl/news/384031_1/Realne.zagrozenia.wirtualizacji.html (23.12.2016).

Kupczyk P., 2011, *Dlaczego bezpieczeństwo wirtualizacji jest istotne dla biznesu?,* http://www.dlp-expert.pl/articles/id,1788/dlaczego_bezpieczenstwo_wirtualizacji_jest_istotne_dla_biznesu.html (12.01.2017).

Luo S., Lin Z., Chen X., 2011, *Virtualization security for Cloud computing service*, IEEE, s. 174-178.

Mendyk-Krajewska T., Mazur Z., Mazur H., 2014, *Konkurencyjność rozwiązań wirtualnych infrastruktury informatycznej*, Zeszyty Naukowe Uniwersytetu Szczecińskiego, nr 809, Ekonomiczne Problemy Usług, nr 113/2014, Wydawnictwo Uniwersytetu Szczecińskiego, Szczecin.

Pomorski S., 2009, *Bezpieczeństwo w środowisku wirtualnym*, Computerworld, 9.02.2009, http://www.computerworld.pl/news/336396/Bezpieczenstwo.w.srodowisku.wirtualnym.html (5.01.2017).

Popek G.J., Goldberg R.P., 1974, *Formal requirements for virtualizable third generation architectures*, Communications of the ACM, vol. 17, iss. 7, s. 412-421, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.141.4815&rep=rep1&type=pdf (10.12.2016).

Porowski D., 2011, *Co to jest wirtualizacja*, Microsoft, http://technet.microsoft.com/pl-pl/library/co-to-jest-wirtualizacja.aspx (5.12.2016).

Przybylak P., 2010, *Wirtualna infrastruktura – nowe podejście do systemów*, Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki, nr 4/2010, http://zeszyty-naukowe.wwsi.edu.pl/zeszyty/zeszyt4/Wirtualna_Infrastruktura_-_Nowe_Podejscie_Do_Systemow.pdf (3.01.2017).

Reuben J.S., 2007, *A Survey on Virtual Machine Security*, Seminar on Network Security, Technical report, Helsinki University of Technology, http://www.tml.tkk.fi/Publications/C/25/papers/Reuben_final.pdf (19.01.2017).

Roszkowski M., 2011, *Wpływ wirtualizacji środowiska informatycznego na funkcjonowanie przedsiębiorstwa,* Studies & Proceedings of Polish Association for Knowledge Management, Polskie Stowarzyszenie Zarządzania Wiedzą Seria: Studia i Materiały, nr 57/2011, http://www.pszw.edu.pl/pl/publikacje/item/984-tomt057-4 (17.01.2017).

Rot A., 2016, *Zarzadzanie ryzykiem w cyberprzestrzeni – wybrane zagadnienia teorii i praktyki*, [w:] *Projektowanie i realizacja systemów informatycznych zarządzania. Wybrane aspekty*, Komorowski T.M., Swacha J. (red.), Polskie Towarzystwo Informatyczne PTI, Warszawa.

Rule D., Dittner R., 2007, *The Best Damn Server Virtualization Book Period*, Syngress Publishing Inc., Burlington.

Scheffy C., 2007, *Virtualization For Dummies*, AMD Special Edition, Wiley Publishing, Inc., New York.

Sobati S., 2013, *A survey of virtualization security*, International Journal of Scientific & Engineering Research, vol. 4, iss. 9, September, http://www.ijser.org/researchpaper/A-survey-of-virtualization-security.pdf (12.01.2017).

Szyjko C.T., 2012, *Innowacyjne zarządzanie w środowisku wirtualnym*, Zarządzanie Innowacyjne w Gospodarce i Biznesie, nr 1(14)/2012, s. 119-129, http://www.ziwgib.ahe.lodz.pl/sites/default/files/ZIwGiBnr1-14-2012.pdf#page=115 (11.01.2017).

Turek T., 2011, *Wybrane aspekty wirtualizacji środowiska informatycznego w przedsiębiorstwach partnerskich*, [w:] Ekonomiczne Problemy Usług nr 67*, Drogi dochodzenia do społeczeństwa informacyjnego. Stan obecny, perspektywy rozwoju i ograniczenia*, t. 1, Zeszyty Naukowe nr 650 Uniwersytetu Szczecińskiego, Babis H., Czaplewski R. (red.), Wydawnictwo Naukowe Uniwersytetu Szczecińskiego, Szczecin.