



Bezpieczeństwo środowisk cloud computing

Zabezpieczenia serwerów



Maszyny wirtualne
w środowiskach
cloud computing

*Dokument White Paper firmy Trend Micro
Sierpień 2009*

I. WPROWADZENIE

Środowiska cloud computing porównuje się do wczesnej fazy elektryfikacji. Gospodarstwa domowe, firmy i miasta nie chciały same jej wytwarzać i polegać na własnych źródłach zasilania. Zaczęły się łączyć w większą sieć energetyczną, która była obsługiwana i kontrolowana przez elektrownie. Takie rozwiązanie pozwoliło na zaoszczędzenie czasu i pieniędzy oraz umożliwiło szerszy i bardziej niezawodny dostęp do energii.

Podobnie środowiska cloud computing stanowią istotną szansę dla usługodawców i dużych przedsiębiorstw. Korzystając z nich, przedsiębiorstwa mogą zaoszczędzić pieniądze oraz zyskać elastyczność i możliwość wyboru zasobów obliczeniowych. Interesują się tym rozwiązaniem, aby zwiększyć wydajność swojej infrastruktury o moc obliczeniową na żądanie.

W tym dokumencie przedstawiono rodzaj środowiska cloud computing określanego też jako rozwiązanie Infrastructure as a Service (IaaS), czyli infrastruktura dostępna jako usługa. Rozważono wyzwania z zakresu bezpieczeństwa i wpływ takiego podejścia na zabezpieczenia oraz zaproponowano najlepsze sposoby postępowania dla usługodawców i dużych przedsiębiorstw, które mają nadzieję wykorzystać technologię IaaS do poprawienia wyników finansowych w tych niepewnych czasach.

II. MOŻLIWOŚCI ŚRODOWISKA CLOUD COMPUTING

Poszukiwanie możliwości zwiększenia konkurencyjności poza organizacją nie jest niczym nowym — to po prostu outsourcing. Skąd więc bierze się takie zainteresowanie środowiskami cloud computing?

Impet branży. Analitycy branżowi i firmy takie jak Amazon, Citrix, Dell, Google, HP, IBM, Microsoft, Sun oraz VMware zdają się jednomyślnie popierać rozwiązania cloud computing. We wrześniu 2008 roku firma VMware ze swoją inicjatywą vCloud dała pierwszy przykład dostawcy technologii łączącego usługodawców, aplikacje i technologie w celu zwiększenia dostępności i szans dla przedsiębiorstw na wykorzystanie takich środowisk.

Elastyczność. Przedsiębiorstwa mają bezprecedensową możliwość uzyskania elastyczności. Mogą zlecić obsługę sprzętu zewnętrznym wykonawcom, zachowując kontrolę nad infrastrukturą informatyczną. Mogą zlecić obsługę wszystkich elementów infrastruktury zewnętrznym wykonawcom. Wdrażają też, często w ramach projektów wewnątrz określonych działów, segmenty infrastruktury, które są w pełni lub częściowo obsługiwane przez zewnętrznych wykonawców.

Terminologia środowisk cloud computing

IaaS: Infrastructure as a Service, czyli infrastruktura dostępna jako usługa, to rozwiązanie, w którym fizyczna infrastruktura składa się z wirtualnych wystąpień wymaganych zasobów. Przykładowi dostawcy: Amazon EC2, GoGrid.

PaaS: Platform as a Service, czyli platforma dostępna jako usługa, to rozwiązanie opisywane przez analityka firmy Redmonk, Stephena O'Grady'ego* jako środowisko „fabric computing”, w którym architektura fizyczna i logiczna są ukryte za warstwą abstrakcji. Przykłady: Google App Engine, Microsoft Azure.

SaaS: Software as a Service, czyli oprogramowanie dostępne jako usługa, polega na udostępnieniu określonych aplikacji za pośrednictwem Internetu. Przykład: Salesforce.com, Workstream.

*<http://redmonk.com/sogrady/topic/cloud>

ŚRODOWISKA CLOUD COMPUTING

MASZYNY WIRTUALNE W ŚRODOWISKACH CLOUD COMPUTING

Oszczędność kosztów. Dostępność infrastruktury na żądanie umożliwia lepsze wykorzystanie wydatków na infrastrukturę informatyczną. Ograniczenia dotyczące zatrudnienia oraz nakładów inwestycyjnych często stanowią barierę dla innowacji. Sezonowe potrzeby powodują wzrost zapotrzebowania na możliwości obliczeniowe i wymagają utrzymywania niezawodnej infrastruktury, która często pozostaje niewykorzystywana. Środowiska cloud computing stanowią ekonomiczną alternatywę.

Mobilność i wybór. Technologia leży u podstaw ewolucji. Technologie wirtualizacji, takie jak te oferowane przez firmę VMware, umożliwiają przeniesienie aplikacji i usług z wewnętrznych środowisk do publicznego otoczenia sieciowego (środowiska cloud computing) lub od jednego usługodawcy do drugiego.

SKALOWALNOŚĆ

Rozwiązanie Infrastructure as a Service (IaaS) stanowi synonim skalowalności. Serwery potrzebne są natychmiast, ale brak czasu na dokonanie zakupu? Aby uzyskać dostęp do infrastruktury na żądanie, wystarczy karta kredytowa. Poszczególne działy oraz małe i średnie firmy (w tym mniejsi usługodawcy oraz usługodawcy specjalizujący się w usługach zarządzanych) potrzebujące mocy obliczeniowej na żądanie mogą skorzystać z zalet rozwiązań cloud computing. Funkcja przejmowania zadań w razie awarii oraz nadmiarowość to kolejne ważne powody do korzystania z tych rozwiązań.

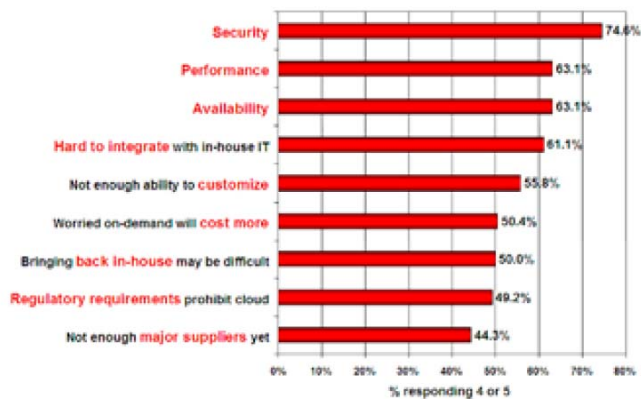
Środowiska cloud computing po prostu ułatwiają przedsiębiorstwom spełnianie wymagań w zakresie możliwości obliczeniowych potrzebnych w codziennej działalności. Zważywszy na elastyczność i możliwość wyboru, mobilność i skalowalność — a wszystko to przy potencjalnej oszczędności kosztów — zastosowanie środowisk cloud computing daje istotne korzyści. Jednak tym, co powstrzymuje organizacje przed przeniesieniem wykonywania ich zadań do publicznych środowisk, jest bezpieczeństwo.

Na przykład firma IDC przeprowadziła ankietę wśród 244 kierowników bądź dyrektorów ds. IT oraz ich współpracowników, aby poznać ich opinie oraz sposób, w jaki ich firmy korzystają z usług cloud computing. Bezpieczeństwo okazało się największym wyzwaniem lub najpoważniejszym problemem związanym z takimi rozwiązaniami.

Jak przenosisz się do środowisk cloud computing?

Przedsiębiorstwa zaczynają korzystać ze środowisk cloud computing na dwa sposoby. Po pierwsze dyrektorzy ds. IT dostrzegają możliwość uzyskania przewagi nad konkurencją, oszczędności kosztów, większej mocy obliczeniowej oraz elastyczności dzięki przejmowaniu zadań w razie awarii i uważają, że są to korzyści zbyt nęcające, aby z nich nie skorzystać. Rozważają zastosowanie takich środowisk i pytają, jak zachować zgodność z regułami zabezpieczeń i spójność w tym nowym, dynamicznym środowisku. Po drugie, działy lub grupy robocze pożądamy natychmiastowego dostępu do zasobów i wyników wdrażają takie środowiska, być może nie zastanawiając się nad bezpieczeństwem przy umieszczeniu aplikacji i danych o kluczowym znaczeniu w środowiskach cloud computing.

Q: Rate the challenges/issues ascribed to the 'cloud'/on-demand model
(1=not significant, 5=very significant)



Source: IDC Enterprise Panel, August 2008 n=244

„Jak dotąd największą troską rodzącą się w związku z usługami cloud computing jest bezpieczeństwo. Klienci obawiają się, że umieszczając najważniejsze firmowe informacje i zasoby informatyczne poza zapora, wystawiają się na atak”.

— Frank Gens, wiceprezes i główny analityk, IDC

III. BEZPIECZEŃSTWO I ZGODNOŚĆ Z PRZEPISAMI W ŚRODOWISKACH CLOUD COMPUTING

Przeniesienie maszyn wirtualnych zawierających aplikacje o kluczowym znaczeniu i poufne dane poza teren firmy do publicznego, współużytkowanego otoczenia sieciowego stanowi źródło wyzwań z zakresu bezpieczeństwa dla organizacji, które polegały na ochronie dostępu do sieci jako podstawowej metodzie ochrony centrów danych. Może też powodować niezgodność z przepisami i naruszać reguły zabezpieczeń. Dyrektorzy ds. IT dostrzegający możliwość zwiększenia konkurencyjności, oszczędność kosztów, większą moc obliczeniową oraz elastyczność zapewnianą przez funkcję przejmowania zadań w razie awarii rozważają zastosowanie środowisk cloud computing i pytają:

- Czy będziemy mieć taką samą kontrolę nad regułami zabezpieczeń aplikacji i usług?
- Czy możemy udowodnić naszej organizacji i klientom, że jesteśmy zabezpieczeni i spełniamy wymagania umów o poziomie świadczenia usług?
- Czy nadal zachowujemy zgodność z przepisami i czy możemy to udowodnić audytorom?

Aby odpowiedzieć na te pytania, należy pokrótce rozważyć bezpieczeństwo w tradycyjnym centrum danych oraz wpływ technologii wirtualizacji, która leży u podstaw rewolucji spowodowanej przez pojawienie się środowisk cloud computing.

BEZPIECZEŃSTWO W TRADYCYJNYCH CENTRACH DANYCH

Wyrażenie „centrum danych” od dawna kojarzy się z potężnymi farmami serwerów ukrytymi za zamkniętymi drzwiami, gdzie elektryczność i chłodzenie były równie ważne dla zapewnienia niezawodności i dostępności danych jak bezpieczeństwo sieci. Zabezpieczenia na obrzeżu sieci to najczęściej stosowany sposób ochrony tradycyjnych centrów danych. Wiąże się to zwykle ze

„W środowisku informatycznym z coraz silniejszą agregacją możliwości obliczeniowych i pamięci masowej w mniejszej liczbie urządzeń fizycznych i centrów danych trudno jest stosować strategię fizycznej segregacji zasobów według stref z urządzeniami filtrującymi ruch i kontrolującymi dostęp do tych stref. Może to doprowadzić do ograniczenia korzyści wynikających ze skali oraz innych zalet konsolidacji w obrębie tej infrastruktury.”

Burton Group, „Network Security in the Real World”, Phil Schacter, Eric Maiwald, październik 2008

stosowaniem zapory, stref zdemilitaryzowanych (DMZ), podziałem sieci na segmenty, systemami wykrywania włamań i zapobiegania im (IDS/IPS) oraz narzędziami do monitorowania sieci.

WIRTUALIZACJA — KATALIZATOR ŚRODOWISK CLOUD COMPUTING

Osiągnięcia w zakresie technologii wirtualizacji umożliwiają przedsiębiorstwom uzyskanie większych możliwości przetwarzania przy użyciu niewykorzystywanych mocy serwerów fizycznych. Rozmiar tradycyjnego centrum danych jest stale zmniejszany, aby oszczędzić koszty oraz ograniczyć negatywny wpływ na środowisko dzięki konsolidacji serwerów. Przedsiębiorstwa i usługodawcy korzystają z wirtualizacji w celu udostępnienia wielu klientom serwerów fizycznych, które wcześniej miały jednego klienta lub jedno zastosowanie.

Przeniesienie maszyn wirtualnych do publicznych otoczeń sieciowych powoduje obejście zabezpieczeń sieci przedsiębiorstwa. W rezultacie bezpieczeństwo wszystkich danych zależy od wspólnych zabezpieczeń na obrzeżu otoczenia sieciowego. Brak możliwości zastosowania fizycznej segregacji i zabezpieczeń sprzętowych w celu ochrony przed atakami prowadzonymi między maszynami wirtualnymi na tym samym serwerze pokazuje, że są potrzebne mechanizmy, które można wdrożyć na serwerze lub w samych maszynach wirtualnych.

Wdrożenie ochrony w samych maszynach wirtualnych umożliwia przeniesienie aplikacji i danych o kluczowym znaczeniu do otoczenia sieciowego.

IV. WYZWANIA Z ZAKRESU ZABEZPIECZEŃ W ŚRODOWISKACH CLOUD COMPUTING

Na pierwszy rzut oka wydaje się, że wymagania z zakresu zabezpieczeń są w przypadku dostawców środowisk cloud computing takie same jak w zastosowaniach tradycyjnych centrów danych — wystarczy zastosować silne zabezpieczenia i nie dopuszczać niewłaściwych osób do środka. Jednak, jak wspomniano wcześniej, fizyczna segregacja i zabezpieczenia sprzętowe nie mogą zapewnić ochrony przed atakami podejmowanymi między maszynami wirtualnymi w obrębie jednego serwera. Aby dostawcy środowisk cloud computing mogli korzystać z zalet wirtualizacji, maszyny wirtualne pochodzące od różnych organizacji muszą korzystać z tych samych zasobów fizycznych. Poniżej omówiono podstawowe zagadnienia, które przedsiębiorstwa powinny rozważyć, planując wdrożenia środowisk cloud computing.

DOSTĘP ADMINISTRACYJNY DO SERWERÓW I APLIKACJI

Jedną z najważniejszych cech środowisk cloud computing jest możliwość samodzielnej obsługi dostępnych mocy obliczeniowych, zwykle przez Internet. W tradycyjnych centrach danych dostęp administracyjny do serwerów jest kontrolowany i ograniczony do połączeń bezpośrednich lub w obrębie terenu firmy. W przypadku

„Byłoby miło, gdyby to nowe podejście do realizacji usług informatycznych było z założenia bezpieczne. Jednak rzeczywistość — pełna ataków i ludzkich błędów — wymaga zastosowania odrębnych zabezpieczeń w celu ochrony korporacji przed zagrożeniami bezpieczeństwa podczas migracji do środowisk cloud computing... Chociaż zabezpieczenia punktów brzegowych będą konieczne do ochrony pozostałych funkcji centrów danych oraz znacznej części korporacji, która nie jest mobilna, do zabezpieczenia usług informatycznych opartych na rozwiązaniach cloud computing będzie potrzebne nowe podejście”.

Gartner, „Cloud-Based Computing Will Enable New Security Services and Endanger Old Ones”, czerwiec 2008

ŚRODOWISKA CLOUD COMPUTING MASZYNY WIRTUALNE W ŚRODOWISKACH CLOUD COMPUTING

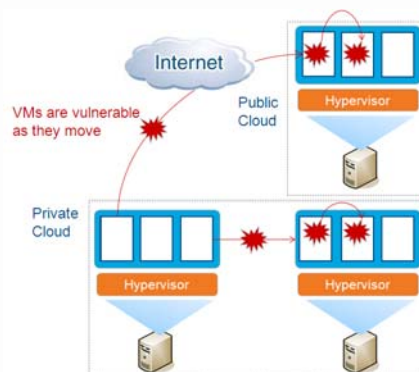
rozwiązań cloud computing czynności administracyjne trzeba wykonywać przez Internet, co zwiększa podatność na atak i ryzyko. Bardzo ważne jest ograniczenie dostępu administracyjnego i monitorowania go w celu zapewnienia przejrzystości zmian w sposobie sterowania systemem.

DYNAMICZNE MASZYNY WIRTUALNE: STAN MASZYN WIRTUALNYCH I ROZPRZESTRZENIANIE SIĘ ZAGROŻEŃ

Maszyny wirtualne są dynamiczne. Można szybko i względnie łatwo przywracać je do poprzedniego stanu, a także wstrzymywać i wznowiać ich pracę. Można je bezproblemowo klonować i przenosić między serwerami fizycznymi. Ten dynamiczny charakter i możliwość rozprzestrzeniania się zagrożeń między maszynami wirtualnymi utrudniają opracowanie i utrzymanie spójnych zabezpieczeń. Luki w zabezpieczeniach lub błędy konfiguracji mogą się niepostrzeżenie propagować. Trudno też utrzymywać rejestr stanu zabezpieczeń maszyny wirtualnej w dowolnej chwili umożliwiający jego skontrolowanie. W środowiskach cloud computing niezbędna jest możliwość zademonstrowania stanu zabezpieczeń systemu niezależnie od jego położenia oraz tego, jak blisko innych, potencjalnie niebezpiecznych maszyn wirtualnych się znajduje.

WYKORZYSTANIE LUK W ZABEZPIECZENIACH ORAZ ATAKI MIĘDZY MASZYNAMI WIRTUALNYMI

Serwery w środowisku cloud computing korzystają z tych samych systemów operacyjnych oraz aplikacji przedsiębiorstw i sieci Web co maszyny wirtualne i serwery fizyczne. Możliwość zdalnego wykorzystania luk w zabezpieczeniach tych systemów i aplikacji przez atakujących lub złośliwe oprogramowanie stanowi poważne zagrożenie dla takich zwirtualizowanych środowisk. Ponadto umieszczenie wielu maszyn wirtualnych obok siebie powoduje zwiększenie obszaru narażenia na atak oraz naruszenie zabezpieczeń między maszynami wirtualnymi. Systemy wykrywania włamań i zapobiegania im muszą mieć możliwość wykrywania złośliwych działań na poziomie maszyn wirtualnych niezależnie od lokalizacji tych maszyn w obrębie zwirtualizowanego otoczenia sieciowego.



ZABEZPIECZANIE UŚPIONYCH MASZYN WIRTUALNYCH

Maszyna wirtualna znajdująca się w trybie offline — w przeciwieństwie do komputerów fizycznych — nadal jest dostępna dla dowolnych aplikacji, które mogą korzystać przez sieć z jej pamięci masowej, i dlatego pozostaje narażona na infekcję złośliwym oprogramowaniem. Jednak uśpione lub wyłączone maszyny wirtualne nie mogą uruchamiać programów wyszukujących złośliwy kod. Uśpione maszyny wirtualne mogą być dostępne nie tylko w technologii hypervisor, ale także mogą być zarchiwizowane w postaci kopii zapasowych na innych serwerach lub nośnikach pamięci masowej. W środowiskach cloud computing odpowiedzialność za ochronę i skanowanie uśpionych maszyn wirtualnych spoczywa na usługodawcy. Firmy korzystające z takich środowisk powinny szukać dostawców umożliwiających zabezpieczenie takich uśpionych maszyn wirtualnych oraz utrzymanie spójnych zabezpieczeń.

WPLÝW TRADYCYJNYCH ZABEZPIECZEŃ NA WYDAJNOŚĆ

Istniejące rozwiązania z zakresu bezpieczeństwa treści zostały utworzone przed pojawieniem się idei wirtualizacji architektury x86 oraz technologii cloud computing. Nie są przeznaczone do pracy w takich

środowiskach. W otoczeniu sieciowym, w którym maszyny wirtualne należące do różnych podmiotów współużytkują zasoby sprzętowe, pełne skanowanie systemu w trakcie pracy może powodować znaczne zmniejszenie wydajności obsługującego je komputera fizycznego. Usługodawcy specjalizujący się w takich środowiskach, którzy udostępniają klientom podstawowe zabezpieczenia, mogą sobie poradzić z tym problemem, wykonując skanowanie wymagające znacznych zasobów na poziomie hypervisor i eliminując w ten sposób rywalizację o zasoby na poziomie hosta.

SPÓJNOŚĆ DANYCH: WSPÓŁWYSTĘPOWANIE, NARUSZENIE ZABEZPIECZEŃ I KRADZIEŻ

Zgodnie z raportem z badania naruszeń zabezpieczeń danych przeprowadzonego w 2008 roku przez zespół oceny ryzyka biznesowego firmy Verizon w 59% przypadków spójność danych została naruszona w wyniku działań hakerskich i włamań do systemów. Oczekuje się, że stosowanie zasobów dedykowanych jest bezpieczniejsze od zasobów współużytkowanych. Obszar narażenia na atak w otoczeniu sieciowym, które jest w całości lub częściowo współużytkowane, jest większy, a zatem wiąże się z nim większe ryzyko. Przedsiębiorstwa potrzebują pewności i dowodów z możliwością kontroli, czy zasoby nie zostały zmienione lub czy nie naruszono zabezpieczeń, zwłaszcza w przypadku korzystania ze współużytkowanej infrastruktury fizycznej. Potrzebne jest monitorowanie plików i działań systemu operacyjnego oraz aplikacji.

SZYFROWANIE I OCHRONA DANYCH

Wiele regulacji i standardów, takich jak PCI DSS czy HIPAA, obejmuje wymóg stosowania szyfrowania w celu ochrony informacji o kluczowym znaczeniu, takich jak dane właściciela karty czy informacje umożliwiające identyfikację, aby zachować zgodność z przepisami lub bezpieczeństwo w przypadku naruszenia zabezpieczeń. Wykorzystywanie środowisk cloud computing przez wielu klientów zwiększa znaczenie tych wymagań i stanowi źródło unikatowych wyzwań związanych z dostępnością i ochroną poświadczeń szyfrowania używanych do ochrony danych.

ZARZĄDZANIE POPRAWKAMI

Możliwość samodzielnej obsługi w środowiskach cloud computing może powodować zamieszanie w zakresie zarządzania poprawkami. Gdy przedsiębiorstwo zasubskrybuje zasób środowiska cloud computing, na przykład tworząc serwer sieci Web z szablonów oferowanych przez usługodawcę, zarządzanie poprawkami do tego serwera należy do obowiązków nie dostawcy środowiska, lecz subskrybenta. Zważywszy że według cytowanego raportu firmy Verizon o naruszeniach danych zabezpieczeń w 2008 roku w przypadku 90% znanych

i wykorzystanych luk w zabezpieczeniach poprawki były dostępne co najmniej 6 miesięcy przed włamaniem, organizacje korzystające ze środowisk cloud computing muszą zachować czujność, aby utrzymać aktualność zasobów w takich środowiskach. Jeśli stosowanie poprawek jest niemożliwe lub nie można tym zarządzać, należy rozważyć zastosowanie środków zastępczych, takich jak „poprawki wirtualne”.

„90% znanych i wykorzystanych luk w zabezpieczeniach zostało poprawionych co najmniej sześć miesięcy wcześniej”.

Raport o naruszeniach zabezpieczeń danych z 2008 roku
Zespół oceny ryzyka biznesowego firmy Verizon

ZASADY I ZGODNOŚĆ Z PRZEPISAMI

Na przedsiębiorstwa są wywierane silne naciski, aby zachowywały zgodność z różnorodnymi regulacjami i standardami, takimi jak PCI, HIPAA czy GLBA, nie wspominając już o praktykach audytów, takich jak SAS70 czy ISO. Przedsiębiorstwa muszą udowodnić, że utrzymują zgodność ze standardami zabezpieczeń niezależnie od położenia systemów — czy są to serwery fizyczne znajdujące się na terenie organizacji, uruchomione na nich maszyny wirtualne czy maszyny wirtualne znajdujące się w środowiskach cloud computing poza organizacją.

OCHRONA NA OBRZEŻU SIECI I STREFY

W przypadku korzystania ze środowisk cloud computing znika ochrona stosowana na obrzeżu sieci przedsiębiorstwa. Bezpieczeństwo wszystkich elementów zależy od wspólnych zabezpieczeń na obrzeżu otoczenia sieciowego. Zapora firmowa, stanowiąca podstawę reguł zabezpieczeń i podziału sieci na strefy, nie sięga serwerów środowiska cloud computing albo jej reguły są kontrolowane nie przez właściciela zasobów, lecz przez dostawcę środowiska. Aby w środowisku cloud computing ustanowić strefy zaufania, maszyny wirtualne muszą same się bronić, co jest równoznaczne z przesunięciem zabezpieczeń na obrzeżu sieci do wnętrza maszyny wirtualnej.

„...nasi klienci już nas nie potrzebują, aby uzyskać dostęp do tych technologii i korzystać z nich. Jednak prawdziwa władza dyrektora ds. IT bierze się z możliwości ułatwienia trwałego przejścia na te technologie”.
Linda Cureton, dyrektor ds. IT, NASA, Centrum lotów kosmicznych w Goddard

BRAK ZABEZPIECZEŃ ZASOBÓW FIRMY

Chcąc natychmiast skorzystać z zasobów i korzyści środowisk cloud computing, takie rozwiązania zaczynają stosować osoby i grupy niezorientowane w tematyce informatycznej. Ważne dane i aplikacje firmowe są wdrażane w otoczeniu sieciowym — możliwe, że bez odpowiednich zabezpieczeń.

V. MASZYNY WIRTUALNE W ŚRODOWISKACH CLOUD COMPUTING

Technologią leżącą u podstaw środowisk cloud computing jest wirtualizacja. Organizacje, które obecnie nie korzystają z takich rozwiązań, prawdopodobnie planują to zrobić. Centra danych ze skonsolidowanymi serwerami fizycznymi i wieloma maszynami wirtualnymi działającymi na serwerach zwirtualizowanych mogą podjąć czynności owocujące natychmiastową poprawą bezpieczeństwa w swoich środowiskach zwirtualizowanych, jak również przygotować te maszyny wirtualne do migracji do środowiska otoczenia sieciowego, gdy okaże się to korzystne.

Poniżej omówiono pięć technologii zabezpieczeń: zaporę, wykrywanie włamań i zapobieganie im, monitorowanie spójności, kontrolę dzienników oraz ochronę przed złośliwym oprogramowaniem, które można wdrożyć w postaci oprogramowania na maszynach wirtualnych w celu poprawienia ochrony i zachowania zgodności z przepisami oraz spójności serwerów i aplikacji podczas przenoszenia wirtualnych zasobów z wnętrza firmy do publicznego otoczenia sieciowego.

ZAPORA

Zmniejszenie obszaru narażonego na atak w przypadku serwerów zwirtualizowanych w środowiskach cloud computing

Dwukierunkowa zaporą nadzorująca stan, wdrożona na poszczególnych maszynach wirtualnych może umożliwić centralne zarządzanie zasadami zapory serwera. Powinna zawierać wcześniej przygotowane szablony dla typowych rodzajów serwerów korporacyjnych i umożliwiać:

- izolację maszyn wirtualnych;
- szczegółowe filtrowanie (według adresów oraz portów źródłowych i docelowych);
- obsługę wszystkich protokołów opartych na protokole IP (TCP, UDP, ICMP i inne);
- obsługę wszystkich typów ramek (IP, ARP i inne);
- zapobieganie atakom typu DoS;
- projektowanie odrębnych reguł dla poszczególnych interfejsów sieciowych;
- wykrywanie skanowania rozpoznawczego na serwerach środowiska cloud computing;
- zmianę działania w zależności od lokalizacji, aby umożliwić zaostrzenie reguł i przeniesienie maszyny wirtualnej z wnętrza firmy do zewnętrznego środowiska.

WYKRYWANIE WŁAMAŃ I ZAPOBIEGANIE IM (IDS/IPS)

Ochrona systemów operacyjnych i aplikacji korporacyjnych przed wykorzystaniem luk w zabezpieczeniach do czasu ich poprawienia w celu zapewnienia szybkiej ochrony przed znanymi i najnowszymi atakami

Jak już wspomniano, maszyny wirtualne i serwery w środowisku cloud computing korzystają z tych samych systemów operacyjnych oraz aplikacji przedsiębiorstw i sieci Web co serwery fizyczne. Wdrożenie na maszynach wirtualnych systemów wykrywania włamań i zapobiegania im w postaci oprogramowania umożliwia ochronę tych aplikacji i systemów operacyjnych przed wykorzystaniem luk w zabezpieczeniach w celu zapewnienia ochrony przed atakami wymierzonymi w maszyny wirtualne. W szczególności reguły dotyczące luk w zabezpieczeniach zapewniają ochronę przed niezliczonymi rodzajami ataków opartych na znanych lukach, na przykład tych ujawnianych co miesiąc przez firmę Microsoft.

MONITOROWANIE SPÓJNOŚCI

Monitorowanie plików, systemów i rejestru pod kątem wprowadzanych zmian

Monitorowanie spójności plików aplikacji i systemu operacyjnego o kluczowym znaczeniu (plików, katalogów, kluczy i wartości rejestru itp.) jest niezbędne w celu wykrywania złośliwych i nieoczekiwanych zmian, które mogą stanowić sygnał naruszenia bezpieczeństwa zasobów środowiska cloud computing. Oprogramowanie do monitorowania spójności musi zostać zastosowane na poziomie maszyny wirtualnej.

Takie rozwiązanie powinno umożliwiać:

- wykrywanie na żądanie lub zaplanowane;

- wszechstronne sprawdzanie właściwości plików, także ich atrybutów (umożliwia osiągnięcie zgodności ze standardem PCI 10.5.5);
- monitorowanie na poziomie katalogów;
- elastyczne, praktyczne monitorowanie przy użyciu reguł uwzględniania i wykluczania;
- tworzenie raportów na potrzeby audytu.

KONTROLA DZIENNIKA

Wgląd w ważne zdarzenia z zakresu bezpieczeństwa pojawiające się w plikach dzienników w zasobach środowiska cloud computing

Kontrola dziennika wiąże się ze zbieraniem i analizowaniem wpisów dziennika systemu operacyjnego i aplikacji dotyczących zdarzeń związanych z bezpieczeństwem. Jej reguły umożliwiają optymalizowanie identyfikacji ważnych zdarzeń ukrytych w wielu wpisach dzienników. Informacje o tych zdarzeniach mogą być wysyłane do niezależnego systemu zabezpieczeń, ale zapewniają największą przejrzystość w przypadku przekazania do systemu zarządzania informacjami i zdarzeniami bezpieczeństwa lub centralnego serwera dzienników w celu zbadania korelacji, zgłoszenia i zarchiwizowania. Podobnie jak w przypadku monitorowania spójności kontrola dziennika musi zostać zastosowana na poziomie maszyny wirtualnej. Oprogramowanie do kontroli dziennika w zasobach środowiska cloud computing umożliwia:

- wykrywanie podejrzanych zachowań;
- zbieranie informacji o działaniach administracyjnych dotyczących bezpieczeństwa;
- zoptymalizowane zbieranie zdarzeń dotyczących bezpieczeństwa z całego centrum danych.

OCHRONA PRZED ZŁOŚLIWYM OPROGRAMOWANIEM W ŚRODOWISKACH WIRTUALNYCH

Eliminacja luk w zabezpieczeniach charakterystycznych dla środowisk zwirtualizowanych i cloud computing

Rozwiązania z zakresu ochrony przed złośliwym oprogramowaniem w środowiskach wirtualnych korzystają z interfejsów API programów typu hypervisor, takich jak interfejsy VMsafe firmy VMware, w celu zabezpieczenia zarówno aktywnych, jak i uśpionych maszyn wirtualnych. Jest to ochrona wielowarstwowa, oparta na użyciu wyspecjalizowanych, skanujących maszyn wirtualnych współpracujących w czasie rzeczywistym z agentami ochrony działającymi na każdej maszynie wirtualnej. Zapewnia to ochronę maszyn wirtualnych w stanie uśpionia oraz gwarantuje pełną aktualizację zabezpieczeń w celu zapewnienia gotowości w momencie wznowienia pracy. Ochrona przed złośliwym oprogramowaniem w środowiskach wirtualnych może zachować wydajność serwerów wirtualnych dzięki uruchamianiu procesów zużywających znaczną ilość zasobów, takich jak pełne skanowanie systemu, z osobnej skanującej maszyny wirtualnej.

- Zapobieganie uruchamianiu złośliwego oprogramowania na aktywnych i uśpionych maszynach wirtualnych.
- Ochrona przed atakami polegającymi na dezinstalacji zabezpieczeń antywirusowych, instalowaniu dla nich nieprawidłowych poprawek lub zapobieganiu ich uruchamianiu.
- Ścisła integracja z konsolami zarządzania wirtualizacją, takimi jak program VMware vCenter.
- Automatyczna konfiguracja zabezpieczeń nowych maszyn wirtualnych.

UWAGI DOTYCZĄCE BEZPIECZEŃSTWA WDROŻEŃ

Wdrożenia w środowiskach cloud computing będą coraz częstsze. Środowiska wirtualne, w których wymienione powyżej mechanizmy zabezpieczeń są stosowane na maszynach wirtualnych, właściwie umożliwiają ich przeniesienie do takich środowisk. Trzy dodatkowe uwagi ułatwią zmaksymalizowanie skuteczności dowolnego wdrożenia zabezpieczeń:

- Agenty oprogramowania uruchamiane na maszynach wirtualnych zapewniają im wyższy poziom bezpieczeństwa. Konsolidowanie mechanizmów ochrony umożliwia realizowanie korzyści ze skali i wdrożeń oraz oszczędność kosztów w przypadku przedsiębiorstw i usługodawców.
- Przedsiębiorstwa raczej nie przeniosą wszystkich działań na zasoby środowisk cloud computing. Wszelkie mechanizmy zabezpieczeń powinny być wdrożone w sposób spójny dla aplikacji na serwerach fizycznych, serwerach wirtualnych i serwerach w środowiskach cloud computing. Te wdrożenia powinny też umożliwiać centralne zarządzanie i integrację z istniejącymi elementami infrastruktury zabezpieczeń, takimi jak narzędzia do integracji rozwiązań wirtualnych (na przykład VMware vCenter), rozwiązania z zakresu zarządzania informacjami i zdarzeniami bezpieczeństwa (na przykład ArcSight, NetIQ i RSA Envision), katalogi przedsiębiorstwa (usługa Active Directory) oraz mechanizmy dystrybucji oprogramowania (takie jak Microsoft SMS, Novel Zenworks oraz Altiris).
- Wiele obecnie wdrożonych narzędzi, takich jak zapory programowe oraz systemy zapobiegania włamaniom oparte na hoście (HIPS), można bezproblemowo przenieść do otoczenia sieciowego. Ponadto w środowiskach wirtualnych i otoczeniu sieciowym można też wdrażać bezpłatne narzędzia i oprogramowanie, takie jak program VM Protection.

VI. WDROŻENIE JUŻ DZIŚ

Stosowanie środowisk cloud computing, podobnie jak w przypadku wszystkich poprzedzających je rozwiązań, wiąże się z ryzykiem i wyzwaniem z zakresu bezpieczeństwa. Nie oznacza to, że należy ich unikać lub opóźniać ich wprowadzanie. Korzyści wynikające z ich stosowania mają zbyt duży potencjał, aby z niego rezygnować.

Firma analizująca możliwość użycia środowiska wirtualnego powinna zbadać wyzwania z zakresu bezpieczeństwa opisane w tym dokumencie i rozważyć następujące zagadnienia:

- Czy środowiska cloud computing są obecnie używane w organizacji? Czy wdrożone aplikacje lub dane mają kluczowe znaczenie dla ciągłości działalności? Czy spełniają wymagania obowiązujących w firmie reguł zabezpieczeń? Czy niepotrzebnie narażają na ryzyko istniejące zasoby firmowe?
- Które stosowane obecnie w sieci firmowej mechanizmy zabezpieczeń nie mogą zostać przeniesione do środowiska cloud computing i jakie wiąże się z tym ryzyko?
- Jaką platformę wirtualizacji oferuje wybrany dostawca środowisk cloud computing? Czy umożliwia ona przedsiębiorstwu swobodne i bezpieczne przenoszenie zasobów ze środowiska i do niego?
- Którego oprogramowania z zakresu bezpieczeństwa można użyć do zapewnienia odpowiedniej ochrony, aby rozpocząć przenoszenie maszyn wirtualnych do otoczenia sieciowego? Narzędzia programowe, takie jak VM Protection, umożliwiają przedsiębiorstwom szybkie zapewnienie ochrony zasobom środowiska cloud computing.

W przypadku usługodawców specjalizujących się w środowiskach cloud computing należy rozważyć następujące zagadnienia:

- Czy platforma wirtualizacji umożliwia przyjmowanie istniejących maszyn wirtualnych klientów korporacyjnych dokonujących migracji istniejących zasobów do otoczenia sieciowego?
- Jak pomaga się klientom w spełnieniu wymagań dotyczących podziału na strefy i segregacji zasobów w otoczeniu sieciowym przy zachowaniu najniższego całkowitego kosztu eksploatacji dzięki maksymalizacji korzyści płynących z pełnego współużytkowania zasobów wirtualnych?
- Jakie mechanizmy zabezpieczeń można wdrożyć lub polecić klientom w celu przygotowania ich maszyn wirtualnych do pracy w środowisku cloud computing?

VII. PODSUMOWANIE

Usługodawcy specjalizujący się w środowiskach cloud computing korzystają z technologii wirtualizacji połączonych z możliwością samodzielnej obsługi, aby zaoferować ekonomiczny dostęp do zasobów obliczeniowych za pośrednictwem Internetu. Aby mogli w pełni korzystać z zalet wirtualizacji, maszyny wirtualne pochodzące od różnych organizacji muszą korzystać z tych samych zasobów fizycznych. Przedsiębiorstwa rozważające możliwość zastosowania środowisk cloud computing w celu rozszerzenia swojej infrastruktury muszą brać pod uwagę wyzwania z zakresu bezpieczeństwa, które mogą doprowadzić do niezgodności z przepisami oraz naruszenia zabezpieczeń aplikacji i danych.

Przeniesienie maszyn wirtualnych do publicznych otoczeń sieciowych powoduje obejście zabezpieczeń sieci przedsiębiorstwa. W rezultacie bezpieczeństwo wszystkich danych zależy od wspólnych zabezpieczeń na obrzeżu otoczenia sieciowego. Brak możliwości zastosowania fizycznej segregacji i zabezpieczeń sprzętowych w celu ochrony przed atakami prowadzonymi między maszynami wirtualnymi na tym samym serwerze pokazuje, że są potrzebne mechanizmy, które można wdrożyć na serwerze lub w samych maszynach wirtualnych.

Wdrożenie mechanizmu ochrony, takiego jak zaporę, system wykrywania włamań i zapobiegania im, monitorowanie spójności, kontrola dziennika i ochrona przed złośliwym oprogramowaniem, w formie oprogramowania instalowanego na maszynach wirtualnych to najskuteczniejsza metoda zachowania spójności, zgodności z przepisami i regułami zabezpieczeń podczas przenoszenia zasobów wirtualnych z wnętrza firmy do publicznego otoczenia sieciowego. Przedsiębiorstwa i usługodawcy wybiegający myślą naprzód wprowadzają tę ochronę na swoich maszynach wirtualnych już dzisiaj, aby uzyskać zabezpieczenia gotowe do pracy w środowiskach cloud computing i skorzystać z zalet tych środowisk przed konkurencją.

Aby uzyskać więcej informacji, można do nas zadzwonić lub odwiedzić naszą witrynę pod adresem <http://emea.trendmicro.com/emea/home/enterprise/>

©2009 Trend Micro, Incorporated. Wszelkie prawa zastrzeżone. Trend Micro i logo t-ball są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy Trend Micro Incorporated. Pozostałe nazwy firm i produktów mogą być znakami towarowymi lub zastrzeżonymi znakami towarowymi odpowiednich właścicieli. Informacje zawarte w niniejszym dokumencie mogą ulec zmianie bez powiadomienia. (WP01_Cloud-Computing_090811_PL)