ŚRODOWISKA WIELOCHMUROWE – MOŻLIWOŚCI I NOWE WYZWANIA W ZAKRESIE BEZPIECZEŃSTWA

ZALETY I ZAGROŻENIA ZWIĄZANE Z DYWERSYFIKACJĄ CHMUR

Dostawcy usług chmurowych są w siódmym niebie – w ciągu zaledwie kilku lat ich branża eksplodowała. Z alternatywnej platformy, z której korzystało kilka odważnych i innowacyjnych firm, przekształciła się w oparty na chmurze standard obsługujący wszelkie kluczowe systemy biznesowe. Według IDC do 2019 roku niemal 50% wydatków na infrastrukturę informatyczną będzie przeznaczanych na chmury publiczne i prywatne.[1]

Obecnie te wydatki idą na bardziej zróżnicowane usługi chmurowe. Według RightScale przedsiębiorstwa korzystają średnio z 1,8 chmury udostępniającej infrastrukturę jako usługę (IaaS).[2] Badania firmy Okta wykazały, że firmy używają średnio 13 aplikacji w modelu Software-as-a-Service (SaaS).[3]

W miarę jak działy informatyczne w coraz większym stopniu korzystają z wielu chmur, specjaliści ds. zabezpieczeń infrastruktury informatycznej muszą zmierzyć się z odpowiedzialnością za aplikacje i przepływy pracy chronione przy użyciu odrębnych zabezpieczeń. Mogą przy tym polegać na umowach o poziom usług podpisanych z dostawcami chmur albo wziąć sprawy w swoje ręce i przyjąć kompleksowe podejście do ochrony wielu używanych w ich firmach chmur. Oparta na otwartych standardach infrastruktura zintegrowanych i adaptacyjnych zabezpieczeń zapewnia kompleksową widoczność i możliwość skoordynowanej reakcji na zagrożenia, pomagając organizacjom maksymalnie wykorzystać możliwości stosowanych środowisk wielochmurowych.

5 NAJWIĘKSZYCH DOSTAWCÓW PUBLICZNYCH INFRASTRUKTUR IAAS[4]

- AWS
- Microsoft Azure
- Google Cloud
- IBM
- Oracle Cloud

10 NAJPOPULARNIEJSZYCH APLIKACJI OFEROWANYCH W MODELU SAAS WEDŁUG UDZIAŁU W RYNKU[5]

- Salesforce
- Microsoft
- Adobe
- SAP
- ADP
- Google
- IBM
- Intuit
- Oracle
- Workday

OPRACOWANIE

OBECNY OBRAZ ŚRODOWISK WIELOCHMUROWYCH

Wielochmurowe środowisko organizacji może obejmować:

- Chmury publiczne i prywatne umożliwiające pracę w modelu platforma jako usługa (PaaS) lub infrastruktura jako usługa (IaaS)
- Chmury publiczne i prywatne hostujące aplikacje dostępne w modelu oprogramowanie jako usługa (SaaS)
- Chmury hybrydowe, które łączą centra danych w siedzibie firmy z usługami chmur publicznych lub prywatnych

Przedsiębiorstwa coraz pewniej czują się w środowiskach obejmujących wiele chmur. Przeprowadzone wśród firm zatrudniających co najmniej 1000 osób badanie wykazało, że 85% respondentów korzysta z chmur hybrydowych (58%), wielu chmur publicznych (20%) lub wielu chmur prywatnych (7%).[6] Zgodnie z ankietą przeprowadzoną przez Fortinet organizacje używają obecnie średnio 62 różnych aplikacji działających w chmurach, co stanowi w przybliżeniu jedną trzecią wszystkich wykorzystywanych przez nie aplikacji.[7]

Takie entuzjastyczne podejście pozostaje jednak w sprzeczności z potencjalnie niewesołą perspektywą, jaka rysuje się przed menedżerami ds. zabezpieczeń infrastruktury informatycznej.

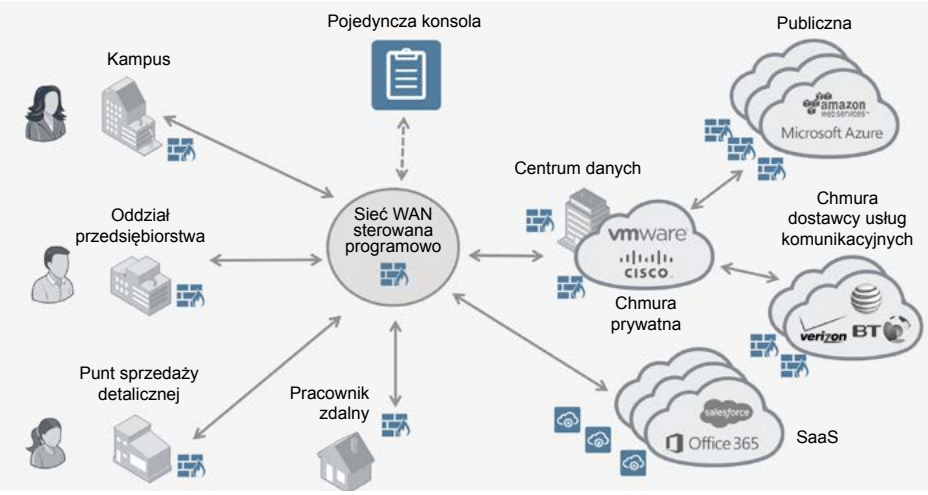
WYZWANIA ZWIĄZANE Z KORZYSTANIEM Z WIELU CHMUR

Migracja do chmur od zawsze była powodowana potrzebą zwiększenia efektywności kosztowej, odporności na awarie i łatwiejszej skalowalności. Wiele chmur oferuje dodatkowe korzyści w postaci możliwości awaryjnego przełączania się na usługi innych usługodawców i unikania uzależnienia od jednego dostawcy.

Korzyści te przestają jednak wydawać się tak atrakcyjne, jeśli weźmiemy pod uwagę kilka problemów związanych z bezpieczeństwem:

Gwałtownie powiększająca się powierzchnia ataku. Jeśli migracja do jednej chmury rozszerza powierzchnię ataku, w przypadku wielu chmur ta powierzchnia zwiększa się w tempie wykładniczym (patrz *Rysunek 1*). W jaki sposób organizacja może skalować zabezpieczenia, by zapewnić ochronę coraz większym i zmieniającym się przepływom pracy realizowanym w wielu chmurach?

Kontrola zagrożeń. Rozdział przepływów pracy na wiele różnych chmur ułatwia rozprzestrzenianie się zagrożeń poza kontrolą organizacji. Typową sprawdzoną metodą ograniczania zagrożeń jest segmentacja, ale w jaki sposób specjaliści ds. zabezpieczeń mogą posegmentować użytkowników i aplikacje działające zarówno w siedzibie firmy, jak i w środowiskach IaaS i SaaS?



RYSUNEK 1. ROZSZERZONA POWIERZCHNIA ATAKU ŚRODOWISKA WIELOCHMUROWEGO.

Odpowiedzialność. Każdy dostawca usług chmurowych odpowiada jedynie za aplikacje i infrastrukturę, które sam udostępnia. Gdy dane – a wraz z nimi wektory ataków – przepływają błyskawicznie między organizacją a różnymi wykorzystywanymi w niej chmurami, w jaki sposób menedżerowie ds. zabezpieczeń infrastruktury informatycznej mogą ustalić źródło ataku? Usługodawcy mogą zwalać winę jedni na drugich, ale w końcu to menedżerowie ds. ochrony odpowiadają przed szefami i udziałowcami firmy.

85%
przedsiębiorstw korzysta z wielu chmur

DLACZEGO ZABEZPIECZENIA CHMUROWE, JAK ZWYKLE, NIE DZIAŁAJĄ W PRZYPADKU WIELU CHMUR

Każdy dostawca usług chmurowych wart swojej ceny inwestuje spore środki w ochronę aplikacji i infrastruktury swoich klientów. Każdy z nich będzie też przekonywał o względnych zaletach stosowanych przez siebie zabezpieczeń. W rezultacie jednak użytkownicy wielu chmur zderzą się z wielością różnorakich technologii ochrony, platform i narzędzi do zarządzania. Przed korporacyjnymi zespołami ds. bezpieczeństwa taka sytuacja stawia kilka wyzwań:

Słaba widoczność. Jako że specjaliści ds. zabezpieczeń infrastruktury informatycznej biorą odpowiedzialność za pełen wachlarz aplikacji i danych korporacyjnych, muszą być w stanie ocenić bezpieczeństwo ich wszystkich. Mają oni oczywiście wgląd w poszczególne chmury przez przeznaczone do tego portale, ale nie zobaczą w ten sposób zagrożeń we wszystkich chmurach (które zazwyczaj nie komunikują się ze sobą) ani nie mogą natychmiastowo ocenić wpływu zagrożeń w jednej chmurze na całą organizację.

Brak koordynacji. Jako że środowiska wielochmurowe przypominają rozgałęziający się model piasty i szprych, specjaliści ds. zabezpieczeń infrastruktury informatycznej mają trudność z jednoczesnym dotarciem do wszystkich używanych chmur w celu wykrycia zagrożeń i zareagowania na nie. Bez integracji między funkcjami zabezpieczeń i scentralizowanej koordynacji nie mogą opracować spójnej reakcji w celu złagodzenia skutków ataku.[8]

Wysoki całkowity koszt posiadania, ochrona reaktywna. Osoby pełniące funkcje CISO bez wątpienia robią, co mogą, ale próbując konsolidować zabezpieczenia środowisk wielochmurowych, generują o wiele wyższe koszty niż w przypadku jednej chmury. Ważny jest przy tym także czas. Przy dzisiejszych zagrożeniach typu zero-day i skracającym się czasie od włamania do naruszenia bezpieczeństwa organizacje nie mogą sobie pozwolić na poświęcanie godzin na zbieranie i dopasowywanie danych z różnych portali do zarządzania chmurami czy porównywanie sygnałów z różnych chmur przed podjęciem decyzji o wymaganych działaniach.

PRZYSZŁOŚĆ ZABEZPIECZEŃ WDROŻEŃ WIELOCHMUROWYCH: KOMPLEKSOWA INFRASTRUKTURA

Sprostanie wyzwaniom, jakie stawiają przed nami środowiska wielochmurowe, wymaga bardziej holistycznego podejścia, które przywróciłoby kontrolę firmowym zespołom ds. bezpieczeństwa. Potrzebny jest przy tym kompleksowy zestaw narzędzi do zapobiegania zagrożeniom, ich wykrywania i łagodzenia ich skutków, które można zintegrować ze wszystkimi głównymi usługami chmurowymi i którymi można zarządzać na miejscu w firmie z jednego pulpitu.

Może to brzmieć jak rozwiązanie platformowe, ale takie nie jest. Platforma to po prostu zestaw powiązanych ze sobą luźno produktów. Infrastruktura zabezpieczeń nie jest produktem, lecz architekturą opartą na otwartych standardach i protokołach, które integrują różne urządzenia ochrony – w tym także platformy – w jeden system zabezpieczeń obejmujący sieć składającą się z wielu chmur. Zamiast odzwierciedlać gwieździstą strukturę sieci wielochmurowej, infrastruktura tworzy sieć zabezpieczeń, w której wszystkie funkcje ochrony mogą się komunikować zarówno między sobą, jak i z centralną konsolą do zarządzania.

Infrastruktura zabezpieczeń zapewnia nie tylko kompleksową widoczność, lecz także całościowy zasięg. Pozwala pracownikom działu bezpieczeństwa zarządzać poprawkami i nadawać im priorytety, szybko identyfikować i blokować włamania, niezależnie od tego, w której części sieci wystąpią, oraz łagodzić ich wpływ na resztę sieci. W końcu, centralnie zarządzana infrastruktura zabezpieczeń umożliwia kompleksową analizę incydentów i zapewnia specjalistom ds. zabezpieczeń infrastruktury informatycznej wyraźny obraz całości ochrony organizacji, który można z czystym sercem zaprezentować zarządowi firmy.

[1] „Growth in Cloud IT Infrastructure Spending Will Accelerate in 2017 Driven by Public Cloud Datacenters and On-Premises Private Cloud Environments", IDC, 13 stycznia 2017 r.

[2] „RightScale 2017 State of the Cloud Report", RightScale, 2017 r.

[3] Chris Burt, „Slack May be Sexier, but Office 365 Most Used Cloud-based Business App", WHIR, 29 marca 2016 r.

[4] „RightScale 2017 State of the Cloud Report", RightScale, 2017 r.

[5] „Microsoft Leads in SaaS Market; Salesforce, Adobe, Oracle and SAP Follow", Synergy Research Group, 31 sierpnia 2017 r.

[6] „RightScale 2017 State of the Cloud Report", dostęp 29 listopada 2017 r.

[7] „Fortinet Threat Landscape Report Q3 2017", dostęp 29 listopada 2017 r.

[8] Matthew Pley, „Securing the Multi-Cloud: It's Harder Than It Looks", SDxCentral, 17 listopada 2017 r.

SIEDZIBA GŁÓWNA
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
Stany Zjednoczone
Tel.: +1.408.235 7700
www.fortinet.com/sales

BIURO SPRZEDAŻY – REGION EMEA
905 rue Albert Einstein
06560 Valbonne
Francja
Tel.: +33 4 8987 0500

BIURO SPRZEDAŻY – REGION APAC
300 Beach Road 20-01
The Concourse
Singapur 199555
Tel.: +65 6513 3730

CENTRALA – AMERYKA ŁACIŃSKA
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel.: +1 954 368 9990

POLSKA
ul. Złota 59
Budynek Lumen II (6 piętro)
00-120 Warszawa
Polska

marca 8, 2018 1:36 PM

wp-multi-cloud-a4