MIKROSEGMENTACJA KONTEKSTOWA NA PLATFORMIE VMWARE NSX DATA CENTER

Ochrona sieci przed poziomym rozprzestrzenianiem się zagrożeń

Nowoczesne aplikacje są złożone, rozproszone i dynamiczne

Każda organizacja stara się znaleźć sposób na prowadzenie działalności w świecie hiperłączności napędzanym przez aplikacje i dane. Nowoczesne aplikacje są dystrybuowane w wielu centrach przetwarzania danych i chmurach oraz dostarczane aż na obrzeża środowiska.

Dzięki wirtualizacji, a także coraz popularniejszym mikrousługom, metodologii DevOps i konteneryzacji, aplikacje można dziś tworzyć i modyfikować szybciej niż kiedykolwiek. Ze względu na rozproszony charakter współczesnych aplikacji i szybkość, z jaką się zmieniają, zachowanie bezpieczeństwa stało się prawdziwym wyzwaniem.

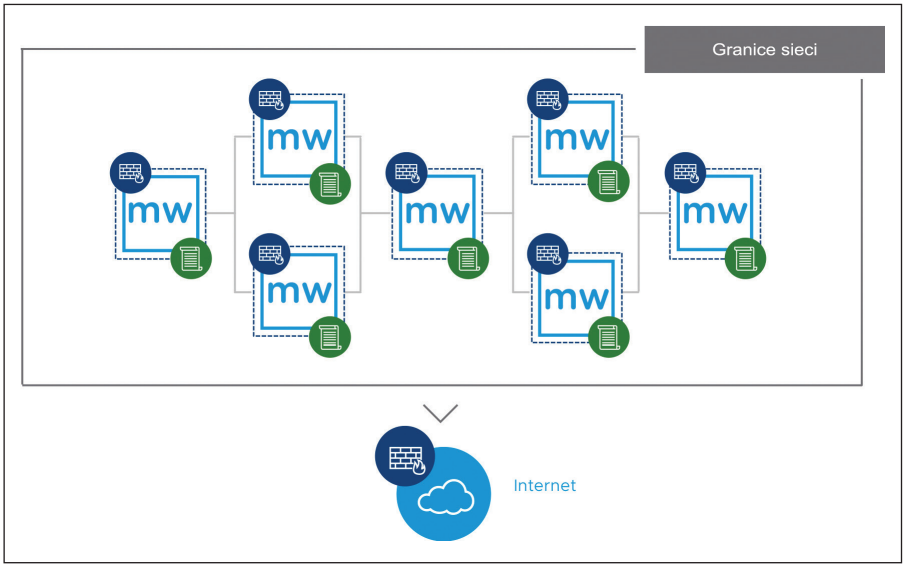
Wcześniejsze strategie zabezpieczeń nie są już skuteczne

Wraz z postępującym rozprzestrzenianiem się aplikacji starsze metody obejmujące stosowanie zabezpieczeń obwodowych okazały się niewystarczające do zapewnienia ochrony aplikacjom i danym. Atakujący niejednokrotnie pokazali, że potrafią złamać lub obejść zabezpieczenia obwodowe. Gdy już dostaną się do środka, bez przeszkód poruszają się w poziomie — od serwera do serwera — poszukując informacji, które można wykraść lub za które można zażądać okupu.

W świecie nowoczesnych, rozproszonych aplikacji zespoły ds. zabezpieczeń IT i sieci często muszą zmagać się z egzekwowaniem odmiennych reguł zabezpieczeń w różnych częściach środowiska, co prowadzi do luk w całym systemie bezpieczeństwa.

Spójne zabezpieczenia dostarczane z centrum przetwarzania danych do chmury i na obrzeża sieci

Na platformie VMware NSX® Data Center można zdefiniować spójny zbiór reguł zabezpieczeń dla całego środowiska, niezależnie od typu aplikacji i miejsca jej wdrożenia. Reguły są egzekwowane na poziomie indywidualnego zadania, co umożliwia segmentację obciążeń realizowanych na tym samym hoście fizycznym bez konieczności ograniczania przepływu ruchu na zewnątrz za pomocą zewnętrznej fizycznej bądź wirtualnej zapory ogniowej. Stosowanie zabezpieczeń na tak szczegółowym poziomie nosi nazwę mikrosegmentacji.



Rysunek 1. Mikrosegmentacja oznacza egzekwowanie zbioru reguł zabezpieczeń sieci na poziomie indywidualnego obciążenia.

„Wraz z rosnącą liczbą urządzeń IoT, im większy jest stopień segmentacji naszej sieci, tym lepiej... W ten sposób zagrożenia nie mogą przemieszczać się poziomo wewnątrz centrum przetwarzania danych”.

CHRISTOPHER FRENZ
DYREKTOR DS. INFRASTRUKTURY
INTERFAITH MEDICAL CENTER

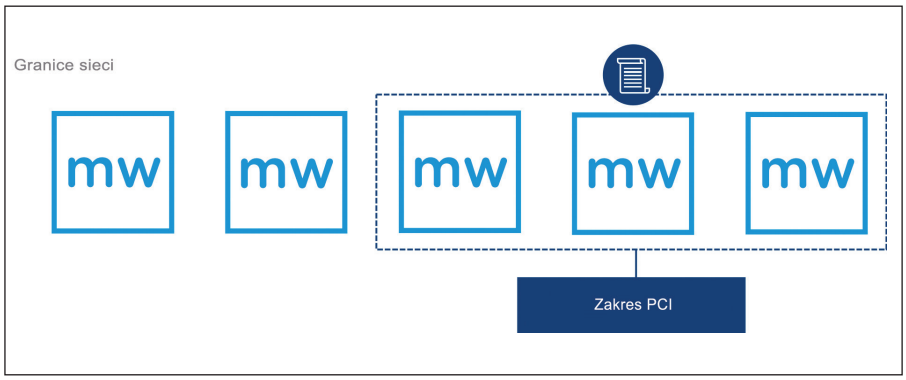
NAJWAŻNIEJSZE INFORMACJE

- Rozproszony, dynamiczny charakter nowoczesnych aplikacji sprawia, że starsze zabezpieczenia obwodowe przestają wystarczać.
- VMware NSX Data Center zapewnia mikrosegmentację, która chroni aplikacje przed poziomym rozprzestrzenianiem się zagrożeń.
- Zbiór reguł zabezpieczeń zdefiniowanych na podstawie kontekstu aplikacji jest egzekwowany indywidualnie dla każdego obciążenia.
- Centrum przetwarzania danych stale dostarcza zabezpieczenia do chmury i na obrzeża sieci.

Mikrosegmenty utworzone na platformie NSX Data Center definiuje się w warstwie oprogramowania i tam też nimi zarządza, co zapewnia ich elastyczność i możliwość automatyzacji. Nowo wdrażane obciążenia automatycznie dziedziczą reguły zabezpieczeń, które pozostają do nich przypisane przez cały cykl życia, niezależnie od miejsca przydzielenia zasobów i ewentualnych przeniesień.

Mikrosegmentacja kontekstowa i zabezpieczenia dopasowane do aplikacji i danych

Możliwość zdefiniowania zbiorów reguł zabezpieczeń na podstawie aspektów najbardziej istotnych w danym środowisku jest równie ważna co spójne egzekwowanie tych reguł. NSX Data Center odłącza reguły zabezpieczeń od statycznych atrybutów sieci, takich jak adres IP, port i protokół, umożliwiając ich definiowanie w oparciu o kontekstowe znaczenie aplikacji i infrastruktury. Konteksty te obejmują atrybuty użytkownika i tożsamości, atrybuty obciążenia (np. system operacyjny), czy nawet zakresy zgodności z przepisami.



Rysunek 2. Mikrosegmenty w NSX Data Center można zdefiniować na podstawie wielu różnych kontekstów, w tym zakresów zgodności z przepisami.

Mikrosegmentacja kontekstowa w NSX Data Center daje zespołom ds. zabezpieczeń elastyczność, która jest niezbędna do zapewnienia bezpieczeństwa aplikacji i danych w oparciu o najważniejsze czynniki. Można na przykład wykorzystać NSX Data Center do zabezpieczenia wdrożenia infrastruktury wirtualnych desktopów (VDI) przez egzekwowanie zbioru reguł sieciowych opartych na kontekście użytkownika na poziomie indywidualnej sesji RDSH. Można tez zastosować zbiór reguł zabezpieczeń do wszystkich obciążeń podlegających standardom branży kart płatniczych (PCI), niezależnie od tego, gdzie fizycznie znajdują się one w środowisku.

Zaawansowane usługi zabezpieczeń w wymaganym miejscu i czasie

NSX Data Center umożliwia wstawianie zaawansowanych zewnętrznych usług zabezpieczeń do danego mikrosegmentu. Zamiast przesyłać cały ruch sieciowy przez urządzenie fizyczne lub instancję wirtualną, takie jak zapora ogniowa nowej generacji (NGFW) lub system wykrywania włamań (IDS) bądź system zapobiegania włamaniom (IPS), NSX Data Center może dynamicznie kierować określony ruch do tych usług w warstwie sieci wirtualnej. W ten sposób można we właściwym momencie wstawić zaawansowane usługi sieciowe w odpowiednich miejscach, maksymalizując efektywność ruchu sieciowego przy jednoczesnym zwiększeniu skuteczności samych usług.

Wgląd w dane o ruchu sieciowym w całym środowisku

Pierwszym krokiem do mikrosegmentacji jest zrozumienie, jak aktualnie wygląda przepływ ruchu w sieci. VMware Network Insight™ zapewnia kompleksowy wgląd w cały ruch sieciowy w centrum przetwarzania danych, co obejmuje ruch w sieci fizycznej i wirtualnej. Po przeanalizowaniu ruchu w sieci VMware Network Insight automatycznie rekomenduje zbiór reguł mikrosegmentacji, który można zastosować na platformie NSX Data Center przy implementacji.

Już dziś skorzystaj z bezpłatnej oceny sieci wirtualnej, aby przeprowadzić analizę bieżącego ruchu w sieci i rozpocząć planowanie projektu mikrosegmentacji. Więcej informacji można uzyskać pod adresem www.vmware.com/pl/products/nsx/security.

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel. 877-486-9273 Faks 650-427-5001 www.vmware.com/pl

Pozycja nr: 147939wf-vmw-q2fy19-sddc-launch-so-nsbu-context-aware-micro-seg-a4
5/18