SIECI SD-WAN W DOBIE TRANSFORMACJI CYFROWEJ

Osiągnięcie sprawności biznesowej bez komplikowania bezpieczeństwa sieci

OPRACOWANIE



STRESZCZENIE

Większość organizacji przechodzi obecnie transformację cyfrową (ang. digital transformation — DX) w takiej czy innej formie: przekształca sposób, w jaki wprowadza produkty i usługi na rynek, a w ostatecznym rozrachunku oferuje wartość dodaną swoim klientom. Inicjatywy związane z DX komplikują jednak także pracę zespołu odpowiedzialnego za działanie sieci. Gdy usługi o krytycznym znaczeniu dla biznesu są rozproszone w wielu środowiskach chmurowych, prowadzi to do potencjalnych problemów związanych z wydajnością, szczególnie w oddziałach.

Jeśli wziąć to wszystko pod uwagę, nie jest zaskoczeniem, że technologia sieci rozległych definiowanych programowo (SD-WAN) błyskawicznie zyskuje popularność. Niestety, rozwiązania SD-WAN są przykładem paradoksu DX: nowa technologia może pomóc firmie osiągnąć kolejny poziom rozwoju, ale jednocześnie poszerza powierzchnię ataku, może więc narazić organizację na znaczne ryzyko. Dlatego też wdrożeniu rozwiązań SD-WAN, tak jak wszystkim innym działaniom związanym z DX, powinna towarzyszyć transformacja zabezpieczeń (ang. security transformation — SX): ponowne przemyślenie przestarzałych zasad, rozszerzenie ochrony poza centrum danych oraz zintegrowanie architektury zabezpieczeń w celu scentralizowania monitorowania i zarządzania.



Transformacja cyfrowa powoduje przenoszenie coraz większej liczby usług do chmury, co powoduje przeciążenie tradycyjnych architektur sieciowych i skłania organizacje do wprowadzenia rozwiązań SD-WAN.

DX WYZNACZA PLAN DZIAŁAŃ

DX jest obecnie prawdopodobnie najważniejszym trendem biznesowym w organizacjach IT. Umożliwia firmom sprawniejsze działanie i szybszą skalowalność, co jest absolutnie niezbędne w wielu branżach[1]. Dzięki DX przedsiębiorstwa wykorzystujące technologie cyfrowe przekształcają się w organizacje w pełni cyfrowe, „ w wysokim stopniu usieciowione, adaptacyjne, inteligentne i sprawne dzięki ścisłemu zintegrowaniu technologii z nowymi procesami operacyjnymi, zasadami i organizacjami, które pozwalają lepiej wykorzystać możliwości w zakresie transformacji”[2].

DX przebiega nieco inaczej w każdej organizacji, ale prawie zawsze oznacza rosnące uzależnienie od architektury chmury hybrydowej. Dla zespołu odpowiedzialnego za działanie sieci oznacza to konieczność połączenia istniejących zasobów znajdujących się w siedzibie firmy z wieloma zewnętrznymi sieciami chmurowymi oraz zapewnienia ich dostępności i wydajności niezależnie od lokalizacji użytkownika.

SD-WAN ODPOWIEDZIĄ NA POTRZEBY DX ZWIĄZANE Z SIECIAMI

W miarę wzrostu liczby usług przenoszonych do chmury staje się coraz bardziej oczywiste, że „konwencjonalne architektury sieciowe (…) nie zostały zbudowane z myślą o obsłudze ruchu w organizacji opartej na chmurze”[3]. To przyczynia się do gwałtownego rozwoju kolejnej technologii kluczowej dla DX: SD-WAN. Użycie słowa „gwałtowny” nie jest tu nadużyciem: badania przeprowadzone przez IHS Markit pokazują, że w 2017 r. 74% firm przeprowadziło testy rozwiązań SD-WAN, a w tym roku wiele z nich wdrożyło tę technologię[4].



SD-WAN zapewnia użytkownikom znajdującym się poza siedzibą główną przedsiębiorstwa wysoko wydajny dostęp do aplikacji w chmurze, umożliwiając zwiększenie sprawności sieci i ułatwiając wprowadzenie automatyzacji w oddziałach w stopniu, jaki wcześniej nie był możliwy. Do szczególnych korzyści należą:

1. **Bezpośredni dostęp do chmury.** Sieć SD-WAN eliminuje konieczność przekierowywania przez centrum danych całego ruchu generowanego przez aplikacje chmurowe i systemy w oddziałach (tzw. backhaulingu). Zapewnia to bezpośredni dostęp do kluczowych usług w chmurze wszystkim użytkownikom, niezależnie od lokalizacji.
2. **Lepsza wydajność aplikacji.** Sieć SD-WAN może zostać skonfigurowana w taki sposób, aby priorytetowo traktować ruch o znaczeniu kluczowym dla działalności biznesowej i usługi czasu rzeczywistego, takie jak VoIP (Voice over Internet Protocol), a także kierować je najbardziej wydajną ścieżką. Dostępność kilku opcji przekierowania ruchu pomaga zmniejszyć liczbę pakietów traconych na przeciążonych łączach oraz opóźnienia wynikające z dużego natężenia ruchu. To zaś wpływa pozytywnie na wydajność całego systemu i na jakość doświadczeń użytkowników[5].
3. **Zwiększona sprawność biznesowa.** Osoby odpowiedzialne za rozwój sieci nie muszą już planować wdrożenia dodatkowego pasma MPLS (Multirotocol Label Switching) w tradycyjnej sieci WAN z kilkutygodniowym czy kilkumiesięcznym wyprzedzeniem. Co więcej, potrzeba zapewnienia wydajności sieci w wielu oddziałach nie hamuje już szybkiego rozwoju innych inicjatyw DX.
4. **Oszczędność kosztów.** Sieć SD-WAN pozwala na efektywne przekierowywanie ruchu przez wiele kanałów: nie tylko istniejące łącza MPLS, ale także publiczne łącza internetowe (LTE i połączenia szerokopasmowe)[6]. To pozwala obniżyć koszty nowych łączy MPLS.

SD-WAN MOŻE TEŻ ZMNIEJSZYĆ BEZPIECZEŃSTWO SIECI

Trudno zaprzeczyć zaletom architektury sieci SD-WAN w świecie DX, ale rozwiązania te mają również jedną bardzo istotną wadę. Każda lokalizacja wykorzystująca sieć SD-WAN z lokalnym dostępem do Internetu stanowi rozszerzenie powierzchni ataku wymierzonego w organizację — i jest kolejnym słabym ogniwem w łańcuchu zabezpieczeń sieciowych. To pogłębia istniejący problem, ponieważ poziom bezpieczeństwa w oddziałach jest często niższy niż w siedzibie głównej jeszcze przed wprowadzeniem rozwiązań SD-WAN.

74% organizacji przeprowadziło w 2017 roku testy sieci SD-WAN, a w tym roku wiele z nich wdraża takie rozwiązania[7].

Oczywiście większość innych wdrożeń technologii inspirowanych DX również zwiększa powierzchnię ataku organizacji, a bezpieczeństwo jest często uważane za najważniejszy czynnik hamujący realizację inicjatyw związanych z DX[8]. Aby odnieść sukces, każdej inicjatywie w zakresie DX — także wdrożeniu sieci SD-WAN — musi towarzyszyć odpowiednia transformacja zabezpieczeń (SX).

SX ZAPEWNIA BEZPIECZEŃSTWO SIECI SD-WAN

SX wymaga ponownego przemyślenia wcześniej ustalonych i stosowanych w przedsiębiorstwie zasad bezpieczeństwa — w tym modelu opartego na ochronie brzegu sieci, którego skuteczność maleje za każdym razem, gdy wprowadzana jest kolejna usługa w chmurze. SX wymaga również, aby bezpieczeństwo było integralną częścią planowania DX, a nie tylko kwestią uwzględnianą dopiero po wdrożeniu nowego rozwiązania. Przy każdej inicjatywie DX zespoły planistyczne i wdrożeniowe powinny kierować się zasadą bezpieczeństwa już na etapie projektowania, „bezpieczeństwa domyślnego".

Jeśli chodzi o wdrażanie sieci SD-WAN, osoby odpowiedzialne za zabezpieczenia i za działanie sieci powinny wspólnie uczestniczyć w procesie decyzyjnym dotyczącym nowego rozwiązania, a w momencie ostatecznego wyboru powinna być już zdefiniowana strategia w zakresie bezpieczeństwa. Zwykle zespoły te działają „silosowo", a czasem wręcz łagodnie konkurują ze sobą[9]. Jeżeli jednak podejmą współpracę, mogą znaleźć strategiczne odpowiedzi na uzasadnione obawy dotyczące bezpieczeństwa w związku z sieciami SD-WAN:

- Zabezpieczenie rozszerzonej powierzchni ataku stworzonej przez inicjatywy DX i samą infrastrukturę SD-WAN[10].
- Zapewnienie, że złośliwe oprogramowanie, które dociera do sieci, nie będzie się w niej rozprzestrzeniać[11].
- Skompensowanie braków wyszkolonego personelu odpowiedzialnego za zabezpieczenia IT w odległych oddziałach.
- Zapewnienie wglądu w całą sieć i scentralizowanego zarządzania bezpieczeństwem dla całego przedsiębiorstwa.



Wdrożenie sieci SD-WAN wymaga transformacji zabezpieczeń: ponownego przemyślenia wcześniej ustalonych i stosowanych zasad bezpieczeństwa przedsiębiorstwa, w tym modelu opartego na ochronie brzegu sieci.

INTEGRACJA JEST KLUCZEM DO SX

Z ostatnich badań wynika, że przeciętna organizacja zarejestrowała w ciągu dwóch lat 20 włamań związanych z cyberatakami, a cztery z nich spowodowały jakieś szkody: utratę danych, przerwy w działaniu systemu lub naruszenie zgodności z przepisami[12]. Część problemu polega na tym, że wykrycie typowego ataku trwa dłużej niż sześć miesięcy (197 dni), co umożliwia napastnikom przemieszczanie się w obrębie organizacji[13]. Większość z tych zagrożeń to zagrożenia zaawansowane, zaprojektowane tak, by ominąć konwencjonalne środki bezpieczeństwa. Jeśli więc sieci SD-WAN i inne inicjatywy w zakresie DX nie zostaną wdrożone w sposób strategiczny, mogą pogłębić problemy związane z takimi zagrożeniami.

Ponieważ organizacje wdrażają SD-WAN jako wsparcie dla DX, muszą zadbać o to, aby uwzględnić w tych inicjatywach SX. Ponieważ ruch sieciowy omija centrum danych, architektura zabezpieczeń sieciowych musi zostać rozbudowana — ale nie można tego osiągnąć poprzez dodawanie do niej systemów silosowych. W prawdziwie bezpiecznym rozwiązaniu SD-WAN zabezpieczenia są zintegrowane z siecią i obejmują wielooddziałowe, rozproszone środowisko korporacyjne. To pozwala na scentralizowanie monitorowania i zarządzania siecią, rzeczywistą automatyzację procesów związanych z bezpieczeństwem, dynamiczne współdzielenie informacji o zagrożeniach (Threat Intelligence) oraz zwiększenie odporności sieci.



20 włamań związanych z cyberatakami — tyle zarejestrowała przeciętna organizacja w ostatnich dwóch latach. W przypadku gdy czas do wykrycia zagrożenia może przekraczać sześć miesięcy, tradycyjny paradygmat bezpieczeństwa przestaje obowiązywać, narażając organizacje na kradzież danych, ataki związane z wymuszaniem okupu (ransomware) oraz przerwy w działaniu systemów.

POMYŚLNE WDROŻENIE SIECI SD-WAN DZIĘKI SX

Sieci SD-WAN to dla organizacji wspaniała możliwość dostarczania oddziałom wymiernej wartości dodanej. Liderzy ds. IT i bezpieczeństwa muszą jednak pamiętać między innymi o następujących aspektach:

- Sieć SD-WAN jest kluczowym elementem składowym DX dla wielu organizacji.
- Wartość biznesowa rozwiązań SD-WAN jest wymierna: pozwalają udostępniać oddziałom środowiska chmurowe, zapewniają wzrost wydajności aplikacji, zwiększają sprawność biznesową i obniżają koszty.
- Sieć SD-WAN powoduje zwiększenie powierzchni ataku, dla wielu organizacji może więc być najsłabszym ogniwem systemu zabezpieczeń.
- SX jest niezbędne do zapewnienia bezpieczeństwa sieci SD-WAN.
- Jeśli chodzi o bezpieczeństwo SD-WAN, kluczowe znaczenie ma integracja.

[1] Michael Krigsman, „Digital transformation and the CIO: Everything you need to know today", ZDNet, 25 maja 2018 r.
[2] Benson Chan, „Digital transformation reimagines everything", Strategy of Things, 7 września 2017 r.
[3] Kelly Ahuja, „A digital-first enterprise needs SD-WAN", Network World, 7 czerwca 2018 r.
[4] Andy Patrizio, „Enterprises are moving to SD-WAN beyond pilot stages to development", Network World, 7 maja 2018 r.
[5] Lee Doyle, „How does SD-WAN manage real-time network performance?", TechTarget SearchSDN, 9 stycznia 2018 r.
[6] „Traditional WANs vs Next Gen SD-WAN", Infosecurity, 12 grudnia 2017 r.
[7] Andy Patrizio, „Enterprises are moving to SD-WAN beyond pilot stages to development", Network World, 7 maja 2018 r.
[8] „Security Implications of Digital Transformation Report", Fortinet, 26 czerwca 2018 r.
[9] Erin O'Malley, „Driving the Convergence of Networking and Security", SecurityWeek, 15 maja 2018 r.
[10] Steve Garson, „Warning: security vulnerabilities found in SD-WAN appliances", Network World, 28 listopada 2017 r.
[11] Lee Doyle, „What are the options for securing SD-WAN?", Network World, 12 lipca 2018 r.
[12] „Security Implications of Digital Transformation Report", Fortinet, 26 czerwca 2018 r.
[13] „Advanced Threats in Financial Services and Retail: A Study of North America & EMEA", Ponemon Institute, 28 maja 2015 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

Copyright © 2018 Fortinet, Inc. Wszelkie prawa zastrzeżone. Fortinet®, FortiGate®, FortiCare®, FortiGuard® oraz niektóre inne znaki są zastrzeżonymi znakami towarowymi spółki Fortinet, Inc. Pozostałe nazwy związane z Fortinet zawarte w niniejszym dokumencie również mogą być znakami towarowymi lub zastrzeżonymi znakami towarowymi Fortinet. Wszelkie inne nazwy produktów lub spółek mogą być znakami towarowymi ich odpowiednich właścicieli. Przedstawione w niniejszym dokumencie parametry wydajności i inne dane uzyskano podczas testów laboratoryjnych w warunkach idealnych, faktyczna wydajność może być zatem inna. Na wartość parametrów wydajności mogą mieć wpływ zmienne sieciowe, różnorodne środowiska sieciowe i inne uwarunkowania. Żadne ze stwierdzeń zawartych w tym dokumencie nie stanowi wiążącego zobowiązania ze strony Fortinet, a Fortinet odrzuca wszelkie wyraźne lub dorozumiane gwarancje i rękojmie, z wyjątkiem gwarancji udzielonych przez Fortinet na mocy wiążącej umowy z kupującym podpisanej przez głównego radcę prawnego Fortinet, w której Fortinet zagwarantuje, że określony produkt będzie działać zgodnie z wyraźnie wymienionymi w takim dokumencie parametrami wydajności, a w takim przypadku wyłącznie określone parametry wydajności wyraźnie wskazane w takiej wiążącej umowie pisemnej będą wiązać Fortinet. Wszelka tego typu gwarancja będzie dotyczyć wyłącznie wydajności uzyskiwanej w takich samych warunkach idealnych, w jakich Fortinet przeprowadza wewnętrzne testy laboratoryjne. Fortinet w całości odrzuca wszelkie wyraźne lub dorozumiane przyrzeczenia, oświadczenia i gwarancje związane z tym dokumentem. Fortinet zastrzega sobie prawo do zmieniania, modyfikowania, przenoszenia lub innego korygowania niniejszej publikacji bez powiadomienia (zastosowanie ma najnowsza wersja publikacji).

15 lutego, 2019 1:28 PM
253349-0-1-PL
wp-sdwan-in-the-age-of-digital-transformation-a4_PL