RESEARCH
Wpływ i zrozumienie dzięki mediom społecznościowym

Grudzień 2016 r.

CISCO ONE – PRZYJAŹNIEJSZE ZABEZPIECZENIA CYFROWE DLA PRZEDSIĘBIORSTW

OFICJALNY RAPORT

Opracowane przez
Zeus Kerravala

ZK Research
Oddział firmy
Kerravala Consulting

O AUTORZE

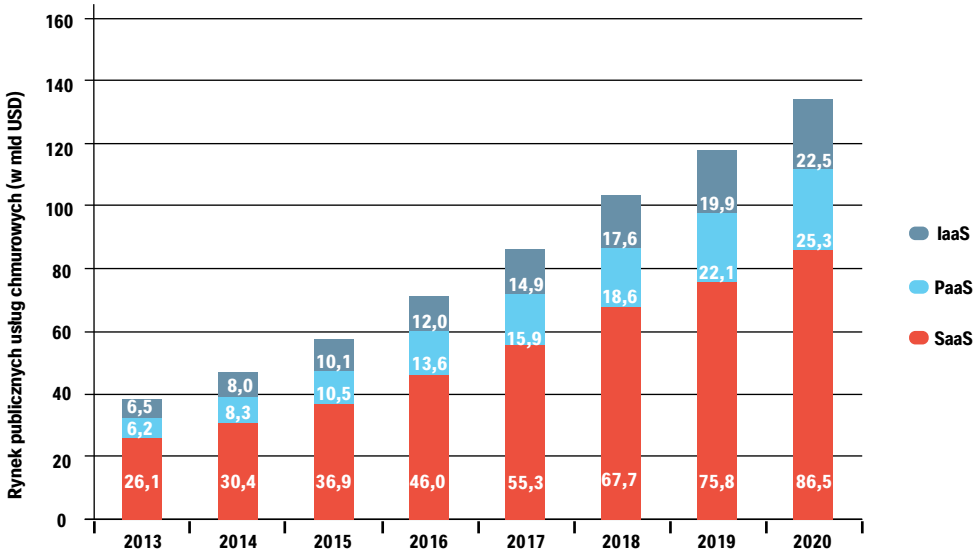
Zeus Kerravala jest założycielem i głównym analitykiem firmy ZK Research. Kerravala świadczy porady o znaczeniu taktycznym i strategicznym, aby pomóc klientom funkcjonować w obecnym klimacie biznesowym i utrzymać swoją działalność w kontekście długoterminowym. Badania i swoją wiedzę oferuje następującym osobom: menedżerom ds. użytkowników końcowych IT i ds. sieci, dostawcom sprzętu, oprogramowania i usług IT, a także przedstawicielom branży finansowej skłonnym inwestować w firmy, którymi się zajmuje.

WPROWADZENIE: CYFROWA DZIAŁALNOŚĆ WYMAGA NOWYCH STRATEGII ZABEZPIECZEŃ

Świat z dnia na dzień staje się coraz bardziej cyfrowy, a środowiska informatyczne firm muszą szybko dostosować się do nowych potrzeb ich działalności. Struktury i działanie sieci definiuje się teraz programowo, aplikacje zostały przeniesione do chmury, pracownicy używają osobistych urządzeń w miejscach pracy, a Internet rzeczy nieustannie zyskuje na popularności. Te zmiany technologiczne zwiększyły dynamiczność i zwinność przedsiębiorstw, pozwalając im szybko reagować na zmieniające się potrzeby rynku. Jedna część ekosystemu IT do tej pory nie uległa jeszcze zmianie – systemy zabezpieczeń. Oto największe zmiany w środowisku IT, które wymagają innego podejścia do bezpieczeństwa:

Erozja barier. Do niedawna wystarczyło postawić zaporę przed łączem internetowym, które jednocześnie stanowiło jedyny punkt dostępu do sieci wewnętrznej, aby zabezpieczyć przedsiębiorstwo. Obecny rozwój technologii przetwarzania w chmurze (Załącznik 1), Internetu rzeczy (IoT) oraz podejścia BYOD (ang. Bring Your Own Device, „przynieś własne urządzenie") doprowadził do erozji istniejących barier sieciowych i stworzył setki potencjalnych punktów dostępu do sieci firmowej. Na przykład – rozwiązania chmury umożliwiają samodzielny zakup usług poszczególnym działom biznesowym. Według badania 2016 Network Purchase Intention Study przeprowadzonego przez firmę ZK Research, 96% organizacji korzysta z usług w chmurze, które nie zostały zakupione przez ich działy IT, a tym samym stanowią martwy punkt dla zespołów ds. zabezpieczeń. Internet rzeczy tworzy coraz więcej martwych punktów, ponieważ punkty odbiorcze IoT są wdrażane przez grupę ds. technologii operacyjnych. Te zmiany poskutkowały otwarciem wielu nowych punktów wejścia do sieci firmowej. ZK Research szacuje, że w ciągu ostatnich 5 lat ich liczba wzrosła dziesięciokrotnie.

Załącznik 1: Gwałtowny rozwój usług chmurowych tworzy nowe zagrożenia dla bezpieczeństwa



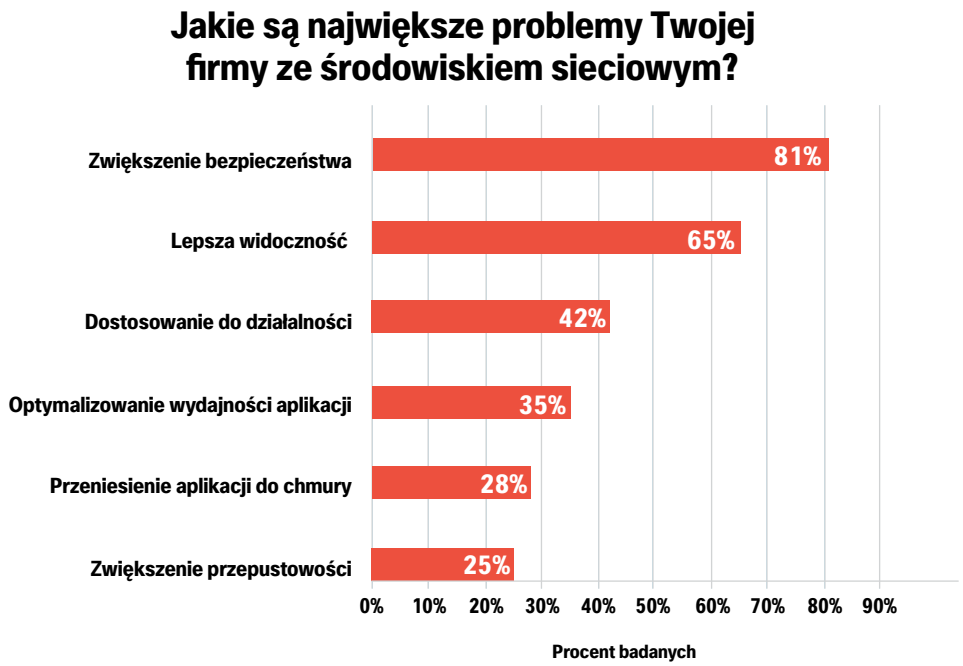
ZK Research 2016 Global Cloud Forecast

Walka z zagrożeniami wymaga ciągłej adaptacji. Według wyników badania 2016 Security Survey wykonanego przez ZK Research, 90% budżetów przeznaczonych na zabezpieczenia wydawanych jest wyłącznie na ochronę punktu zetknięcia sieci lokalnej z zewnętrzną. Jednak tylko 20% wszystkich ataków koncentruje się na tym punkcie. Firmy muszą skoncentrować się na zapobieganiu nowym rodzajom zagrożeń, takim jak phishing, podsłuchiwanie ruchu sieciowego, a także ataki wykorzystujące urządzenia mobilne lub błędy w oprogramowaniu. Cyfrowa transformacja działalności zwiększyła atrakcyjność cyberataków, co oznacza, że zagrożenia będą się mnożyć wykładniczo.

Systemy zabezpieczeń stają się coraz bardziej skomplikowane. Rosnąca liczba punktów wejścia oraz nowych, coraz bardziej wyszukanych metod ataku zmusiła organizacje do wdrożenia większej liczby produktów zabezpieczających w różnych miejscach swojej sieci. Według badania 2016 Security Survey przeprowadzonego przez ZK Research, duże przedsiębiorstwa przeciętnie korzystają jednocześnie z rozwiązań pochodzących od 32 dostawców. Rekordziści korzystają z produktów podchodzących od ponad 100 dostawców. Jednak większa liczba narzędzi zabezpieczających utrudnia utrzymywanie jednolitych zasad zabezpieczeń, a tym samym może paradoksalnie przyczyniać się do pogorszenia jakości systemu zabezpieczeń. Ponadto firma ZK Research odkryła, że naruszenia bezpieczeństwa są zwykle wykrywane po ponad 100 dniach. Mimo wielomiliardowych wydatków przedsiębiorstw na nowe produkty, bezpieczeństwo wciąż pozostaje największym problemem menadżerów ds. sieci (Załącznik 2). Ponadto duża liczba produktów zabezpieczających zainstalowana na punktach końcowych znacząco utrudnia i spowalnia wprowadzanie nawet najmniejszych zmian w całym systemie zabezpieczeń, ponieważ każda zmiana wymaga skonfigurowania i przetestowania wielu rożnych urządzeń. Takie podejście jest również podatne na błędy i może skutkować powstawaniem obszarów bardziej narażonych na ataki.

Firmy coraz śmielej wkraczają w cyfrowy świat. Jednak bieżąca sytuacja na rynku zabezpieczeń jest nadmiernie skomplikowana, a obecne metody są zbyt powolne. Nadszedł czas, aby wszystkie organizacje – od największych przedsiębiorstw po najmniejsze firmy – przeprojektowały swoje strategie zabezpieczeń i dostosowały je do realiów ery cyfrowej.

Załącznik 2: **Bezpieczeństwo pozostaje największym problemem większości organizacji**



ZK Research 2016 Network Purchase Intention Study

CZĘŚĆ II: POZNAJ MODEL OPROGRAMOWANIA CISCO ONE

Cyfrowe organizacje są oparte na technologiach sieciowych, takich jak IoT, przetwarzanie w chmurze oraz mobilność. Znaczenie sieci wzrosło, wymuszając stworzenie struktur sieciowych o większych i bardziej różnorodnych możliwościach. W efekcie procesy zakupu, wdrożenia i obsługi oprogramowania sieciowego stały się bardziej skomplikowane. Ta sytuacja ujawniła szereg wad dotychczasowego procesu obsługi i zakupu oprogramowania sieciowego.

Rosnąca złożoność procesu zamawiania i obsługi licencji na oprogramowanie dla urządzeń sieciowych utrudnia zapewnienie dostępności potrzebnych elementów sieci w odpowiednich miejscach.

Uaktualnienia oprogramowania wdrażane są podczas modernizacji sprzętu, więc nowe funkcje nierzadko trafiają do organizacji zbyt późno, aby zapewnić największe korzyści.

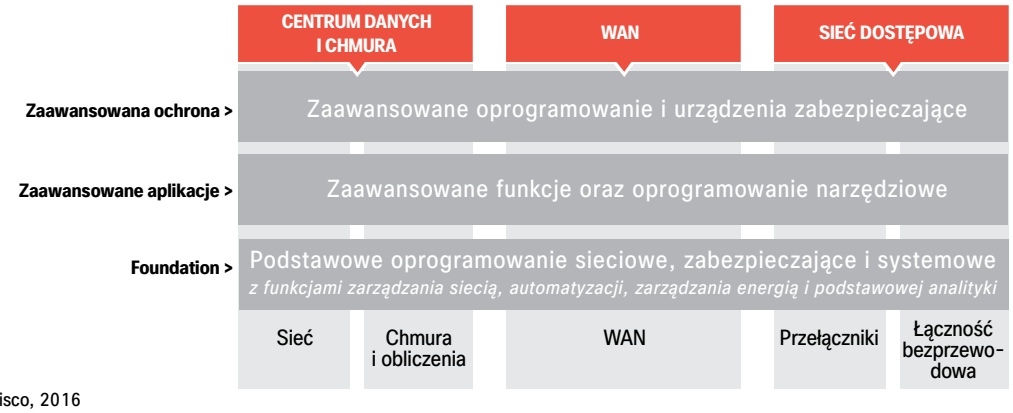
Okresowa modernizacja infrastruktury sieciowej powoduje duże, nagłe wzrosty w wydatkach, utrudniając zarządzanie budżetem.

Oprogramowanie Cisco ONE Software stanowi proste i wszechstronne rozwiązanie do zakupu oprogramowania dla centrów danych, sieci WAN oraz sieci dostępowych. Ten model rozdziela proces zakupu oprogramowania od procesu zakupu platform sprzętowych dla tego oprogramowania.

Oprogramowanie Cisco ONE upraszcza proces zarządzania siecią i zakupu zasobów sieciowych, pozwalając firmom nabyć pakiet z kompletem funkcji i włączyć tylko te elementy, które są w danym momencie potrzebne. Klienci zyskują wiele korzyści, w tym m.in. efektywniejszy proces zakupowy, ochronę inwestycji, dostęp do nowych funkcji oraz wszechstronne modele zakupów.

Oprogramowanie Cisco ONE zostało podzielone na trzy oddzielne domeny: centra danych i chmury, sieci WAN oraz sieci dostępowe. W każdej z tych domen są dostępne trzy różne pakiety funkcji: Foundation, Advanced Applications i Advanced Security (Załącznik 3). Szczegółowe informacje na temat oprogramowania Cisco ONE dla poszczególnych domen można znaleźć pod adresem *www.cisco.com/go/one*.

Załącznik 3: Oprogramowanie Cisco ONE zapewnia użytkownik pełny zakres możliwości



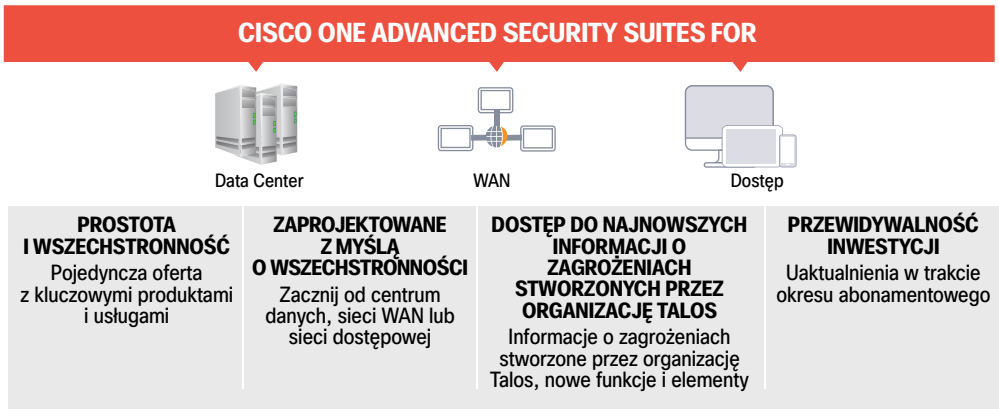
Cisco, 2016

CZĘŚĆ III: OPROGRAMOWANIE CISCO ONE ADVANCED SECURITY

Pakiet Cisco ONE Advanced Security (Załącznik 4) zwiększa możliwości oprogramowania Cisco ONE o funkcje zaawansowanej ochrony. Pakiet ułatwi ufortyfikowanie centrum danych lub sieci WAN organizacji za pomocą prostych w użyciu, przyjaznych w zakupie wstępnie skonfigurowanych pakietów najważniejszych produktów i usług zabezpieczeń.

Klienci, którzy zakupią pakiet zaawansowanej ochrony Cisco ONE otrzymają następujące korzyści:

Załącznik 4: Mechanizmy zaawansowanej ochrony Cisco ONE



ZK Research and Cisco, 2016

Prostota i wszechstronność: Do każdej domeny (centrum danych, sieć WAN i sieć dostępowa) można dokupić wyspecjalizowany pakiet Cisco ONE zawierający niezbędne produkty i usługi zabezpieczeń. Na przykład pakiet dla domeny centrum danych zawiera funkcje zaawansowanej

Większość organizacji koncentruje się na ochronie punktów styku z siecią zewnętrzną, ale często nie zwraca uwagi na wewnętrzne bezpieczeństwo centrum danych.

ochrony przed złośliwym oprogramowaniem i filtrowania adresów URL, nową generację zabezpieczeń przed włamaniami oraz zwirtualizowaną zaporę i powiązane usługi.

Wbudowana elastyczność: Klienci mają pełną swobodę we wdrożeniach i mogą na przykład zdecydować się tylko na jedną konkretną domenę. Jednak klienci, którzy wdrożą pakiety Cisco One Advanced Security we wszystkich trzech domenach odkryją, że całość rozwiązania ma większą wartość niż suma wszystkich jego składników. Rozwiązanie Cisco ONE obsługuje zarówno urządzenia fizyczne, jak i wirtualne (obecnie tylko w domenie sieci dostępowej; obsługa obu rodzajów urządzeń w domenach centrum danych i sieci WAN zostanie wprowadzona wkrótce).

Dostęp do najnowszych informacji o zagrożeniach: Klienci otrzymują dostęp do Cisco Talos, czołowej w branży organizacji do informowania o zagrożeniach, która wspiera funkcje dostępne w produktach Cisco ONE. Pakiet Cisco ONE Advanced Security zapewnia też dostęp do nowych funkcji i możliwości.

Przewidywalność inwestycji: Wszystkie trzy oferty są dostępne w formie abonamentów na okres jednego, trzech lub pięciu lat. Abonamenty zapewniają przewidywalność przepływów pieniężnych. Klienci mogą również uaktualnić abonament i nabyć nowsze urządzenie w trakcie okresu abonamentowego, otrzymując pulę środków za niewykorzystaną część starszego okresu.

Wszystkie abonamenty obejmują usługi wsparcia technicznego dla oprogramowania, w ramach których klienci otrzymują aktualizacje i uaktualnienia oprogramowania, a także dostęp do pomocy technicznej oraz nowych funkcji programu.

Rozwiązania Cisco wyróżniają się na tle rozwiązań innych dostawców, ponieważ obejmują one więcej miejsc w sieci (centrum danych, sieć WAN i sieć dostępową), a także zapewniają szereg zabezpieczeń działających wewnątrz i na zewnątrz firmowej sieci lokalnej.

Aby pomóc klientom w pełni wykorzystać korzyści płynące z oprogramowania Cisco ONE, Cisco oferuje zestaw profesjonalnych usług złożonych z następujących komponentów:

Usługi Quick Start są dostosowane do oprogramowania Cisco ONE i pozwalają na szybkie zintegrowane nowych funkcji w działalności firmy. Inżynierowie ds. usług służą profesjonalną radą i pomocą podczas całego procesu, obniżając ryzyko klientów i jednocześnie skracając czas do uzyskania korzyści. Pakiet Quick Start obejmuje rozruch nowych usług, instalację oprogramowania, konfigurację, dostosowanie produktów do potrzeb klienta, automatyzację zadań, migrację, a także dodawanie i testowanie zasobów.

Usługi optymalizacyjne obejmują zarządzanie zmianami i wprowadzanie nowych rozwiązań. Dzięki tym usługom klienci będą mogli uzyskać pożądany efekt transformacyjny oraz osiągnąć wyznaczone wyniki biznesowe.

CZĘŚĆ IV: CISCO ONE ADVANCED SECURITY FOR DATA CENTER

Centrum danych to serce większości organizacji. To miejsce, w którym przechowywane są wszystkie najważniejsze aplikacje, dane, oraz własność intelektualna firmy. W efekcie centrum danych jest atrakcyjnym celem dla hakerów. Ochrona tego miejsca bywa niełatwym zadaniem, ponieważ niektóre ataki są przypuszczane bezpośrednio z pomieszczenia centrum danych lub przez „tylne drzwi", na przykład przez niezabezpieczony system z dostępem do centrum danych. Większość organizacji koncentruje się na ochronie punktów styku z siecią zewnętrzną, ale często nie zwraca uwagi na wewnętrzne bezpieczeństwo centrum danych. Z danych zawartych w badaniu

2016 Security Survey przeprowadzonym przez ZK Research wynika jasno, że organizacje powinny skoncentrować się na zabezpieczeniach centrów danych:

Obecnie 90% budżetów zabezpieczeń służy do ochrony punktów styku z siecią zewnętrzną, mimo że jedynie 20% ataków jest skoncentrowanych na tych punktach.

Włamania do centrum danych są zwykle wykrywane po 100 dniach.

Ruch „wschód-zachód" stanowi obecnie 70% całego ruchu w centrach przetwarzania danych. Ten rodzaj ruchu omija zabezpieczenia znajdujące się w rdzeniu sieci.

53% badanych osób wyłącza funkcje zabezpieczeń w punktach styku z siecią zewnętrzną w celu uzyskania większej wydajności, dodatkowo narażając centrum danych na atak.

Rozwiązania Cisco ONE Advanced Security for Data Center pozwolą odeprzeć obecne zagrożenia bezpieczeństwa centrum danych:

Pozwalają one tworzyć segmentowane zasady w ramach zwirtualizowanej zapory.

Zawarte w nich mechanizmy zapobiegania atakom następnej generacji pomagają unieszkodliwić zarówno znane, jak i nieznane zagrożenia, bądź całkowicie ich uniknąć.

Funkcje zaawansowanej ochrony przed złośliwym oprogramowaniem pozwalają wykrywać i blokować ukryte złośliwe oprogramowanie oraz ataki typu „zero-day".

Funkcje filtrowania umożliwiają przeanalizowanie ponad 280 milionów stron według reputacji i ponad 80 kategorii.

Zaawansowana ochrona zabezpiecza zarówno zewnętrzne, jak i wewnętrzne obszary sieci przedsiębiorstw, ponieważ coraz więcej ataków ma swoje źródło wewnątrz organizacji.

W Załączniku 5 wyszczególniono wszystkie funkcje zawarte w pakiecie Cisco ONE Advanced Security for Data Center.

Załącznik 5: Cisco ONE Advanced Security for Data Center

ABONAMENTY	SZCZEGÓŁOWE LICENCJE	SPRZĘT (Sprzedawane oddzielnie)
Abonamenty ASA 5585-X*	ASA 5585-X Firepower (IPS, URL, AMP) Kontekst zabezpieczeń	Urządzenie ASA 5585-X
Abonamenty Firepower 4100/9300*	Firepower 9300/4100 Firepower Threat Defense (IPS, URL, AMP)	Urządzenie Firepower 9300/4100

*Abonament obejmuje licencje na oprogramowanie oraz pomoc techniczną, w ramach której klient otrzymuje takie korzyści, jak aktualizacje oprogramowania i sygnatur, pulę środków na uaktualnienia systemów w trakcie okresu abonamentowego oraz dostęp do najnowszych informacji o zagrożeniach oraz funkcji.

Cisco, 2016

CZĘŚĆ V: CISCO ONE ADVANCED SECURITY FOR THE WAN AND EDGE

Dla wielu organizacji najważniejszą częścią działalności są ich oddziały. ZK Research szacuje, że 84% pracowników wszystkich firm pracuje w oddziałach. To właśnie tam wykonuje się większość pracy i obsługuje klientów przedsiębiorstwa. Rosnąca liczba pracowników w oddziałach znacznie wpłynęła na kształt sieci w przedsiębiorstwach. To konsekwencja gwałtownego wzrostu liczby własnych urządzeń podłączonych do sieci – efekt podejścia BYOD. Badanie 2016 Consumerization Survey przeprowadzone przez ZK Research wykazało, że 82% organizacji posiada ustanowiony formalny plan BYOD, a każdy pracownik oddziału ma przy sobie średnio trzy urządzenia. Urządzenia konsumenckie w miejscach pracy stanowią nowe zagrożenia bezpieczeństwa. 75% przedsiębiorstw biorących udział w badaniu 2016 Security Survey przeprowadzonym przez ZK Research podało bezpieczeństwo urządzeń mobilnych jako największy problem w tym kontekście.

Utrzymanie bezpieczeństwa jest też dodatkowo utrudnione przez rosnącą liczbę aplikacji opartych na technologii chmury stosowanych w oddziałach. Aby usprawnić działanie oprogramowania świadczonego jako usługa (SaaS), firmy zapewniają pracownikom możliwość korzystania z chmury bezpośrednio z oddziału, bez przechodzenia przez sieć WAN. Połączenie urządzeń konsumenckich oraz aplikacji w chmurze poskutkowało pięciokrotnym zwiększeniem liczby punktów wejścia do oddziału w ciągu ostatniego roku.

Dlatego systemy zabezpieczające oddziały muszą dotrzymywać kroku cyfrowym realiom. Zabezpieczenia dla oddziałów muszą więc zapewniać:

Bezpieczny dostęp zdalny

Ujednoliconą ochronę połączeń przewodowych i bezprzewodowych

Ochronę danych przed nieupoważnioną modyfikacją, nieautoryzowanym dostępem i podsłuchem

Bezpośredni, bezpieczny dostęp do Internetu

Cisco ONE Advanced Security: Zabezpieczenie przed zagrożeniami dla sieci WAN oraz krawędzi sieci WAN (Threat Defense for WAN and Edge) to rozwiązanie, które zapewnia zaawansowaną ochronę w oddziałach, w tym:

Bezpieczny dostęp zdalny i VPN dla klientów.

Mechanizmy zapobiegania atakom następnej generacji pomagają unieszkodliwić zarówno znane, jak i nieznane zagrożenia, bądź całkowicie ich uniknąć.

Funkcje zaawansowanej ochrony przed złośliwym oprogramowaniem pozwalają wykrywać i blokować ukryte złośliwe oprogramowanie oraz ataki typu „zero-day".

Funkcje filtrowania umożliwiają przeanalizowanie ponad 280 milionów stron według reputacji i ponad 80 kategorii.

W Załączniku 6 przedstawiono strukturę pakietu Cisco ONE Advanced Security: Threat Defense for WAN and Edge.

Załącznik 6: Cisco ONE Advanced Security: Zabezpieczenie przed zagrożeniami dla sieci WAN oraz krawędzi sieci WAN

ABONAMENTY	SZCZEGÓŁOWE LICENCJE	WYMAGANY SPRZĘT (Sprzedawane oddzielnie)
Abonamenty ASA 5500-X*	ASA 5500-X Firepower (IPS, URL, AMP), AnyConnect Plus	Urządzenia ASA 5506, 5508, 5516, 5525, 5545, 5555

*Abonament obejmuje licencje na oprogramowanie oraz pomoc techniczną, w ramach której klient otrzymuje takie korzyści, jak aktualizacje oprogramowania i sygnatur, pulę środków na uaktualnienia systemów w trakcie okresu abonamentowego oraz dostęp do najnowszych informacji o zagrożeniach oraz funkcji.

Cisco, 2016

CZĘŚĆ VI: CISCO ONE ADVANCED SECURITY FOR ACCESS

Struktura krawędzi sieci dostępowej przedsiębiorstwa staje się coraz bardziej złożona. Rosnąca liczba urządzeń konsumenckich oraz aplikacji w chmurze stworzyła wiele martwych punktów, które stanowią zagrożenia dla bezpieczeństwa sieci. Sytuację dodatkowo pogarsza rosnąca popularność Internetu rzeczy (IoT) – coraz więcej nowych urządzeń, takich jak kamery monitoringu, oświetlenie LED, czy systemy klimatyzacji bądź wyspecjalizowane urządzenia różnych działów, łączy się bezpośrednio z krawędzią sieci dostępowej przedsiębiorstwa. Według badania 2016 Network Purchase Intention Study przeprowadzonego przez firmę ZK Research, 70% menedżerów nie jest w stanie precyzyjnie określić liczby wszystkich urządzeń podłączonych do krawędzi sieci dostępowej.

Ponadto cyberprzestępcy zaczęli koncentrować swoje ataki na użytkownikach końcowych oraz aplikacjach, stosując rozbudowane złośliwe oprogramowanie oraz misternie przygotowywane kampanie phishingowe. Gdy takie zagrożenia dostaną się do sieci, pozostają w ukryciu przez kilka miesięcy, zbierając informacje i przygotowując się do wysłania wartościowych danych do atakującego. Na podstawie badania 2016 Security Survey przeprowadzonego przez ZK Research zebrano również inne, równie interesujące statystyki:

90% wszystkich organizacji zostało skutecznie zaatakowanych – z czego 46% tylko w zeszłym roku.

50% firm używa urządzeń mobilnych zainfekowanych złośliwym oprogramowaniem.

Włamania na poziomie warstwy dostępu są zwykle wykrywane po 100 dniach.

96% organizacji używa oprogramowania, które nie zostało zatwierdzone przez IT.

Pracownicy używają średnio czterech aplikacji konsumenckich w toku wykonywania obowiązków na swoim stanowisku.

Firmy potrzebują uproszczonego podejścia do zabezpieczeń krawędzi sieci dostępowej.

Firmy potrzebują uproszczonego rozwiązania zabezpieczającego krawędź sieci dostępowej, dzięki któremu jej pracownicy mogliby uzyskać dostęp do potrzebnych informacji w dowolnym momencie, na dowolnym urządzeniu i z dowolnego miejsca. Natomiast zespoły ds. zabezpieczeń potrzebują lepszej widoczności, aby móc wykryć niecodzienny ruch sieciowy mogący sygnalizować atak.

Cisco ONE Advanced Security: Policy and Threat Defense for Access służy do zwiększania zabezpieczeń i zapewnienia użytkownikom poprawnego i uproszczonego dostępu. Pakiet ten zapewnia:

Wysoce bezpieczny dostęp oparty na identyfikacji użytkownika oraz urządzenia, a także scentralizowany, oparty na tożsamości i kontekście dostęp z dowolnego miejsca

Obsługa widoczności, zgodności oraz zarządzania urządzeniami mobilnymi (MDM)

VPN oraz wysoce bezpieczne punkty końcowe z oprogramowaniem Cisco AnyConnect Apex

W Załączniku 7 przedstawiono strukturę pakietu Cisco ONE Advanced Security: Policy and Threat Defense for Access.

Załącznik 7: Cisco ONE Advanced Security: Policy and Threat Defense for Access

ABONAMENTY	SZCZEGÓŁOWE LICENCJE	WYMAGANY SPRZĘT (Sprzedawane oddzielnie)
Abonamenty ISE i AnyConnect*	ISE-Apex, ISE-Plus, AnyConnect Apex	Urządzenie ISE

*Abonament obejmuje licencje na oprogramowanie oraz pomoc techniczną, w ramach której klient otrzymuje takie korzyści, jak aktualizacje oprogramowania i sygnatur, pulę środków na uaktualnienia systemów w trakcie okresu abonamentowego oraz dostęp do najnowszych informacji o zagrożeniach oraz funkcji.

Cisco, 2016

CZĘŚĆ VII: WNIOSKI I ZALECENIA

Działalność biznesowa wkroczyła w erę cyfrową, razem z którą nadeszły takie technologie, jak IoT, chmura oraz mobilność. Dzięki tym technologiom organizacje stały się bardziej dynamiczne i rozproszone, zyskując nowe poziomy wydajności i efektywności. Firmy, które mogą szybko przejść na cyfrowy model biznesowy, zwiększą swoją rentowność i zyskają przewagę nad konkurencją. Podmioty, które pozostaną przy starym modelu, będą walczyły o przetrwanie.

Jednak te technologie kosztują. Rozwiązania zabezpieczeń stają się coraz bardziej złożone. Tradycyjne metody zabezpieczeń, koncentrujące się na samym obrębie sieci, już nie wystarczają, ponieważ większość ataków omija ten obręb. Architektury zabezpieczeń muszą ulec zmianie, koncentrując się na sieci wewnętrznej, a zwłaszcza na centrum danych, oddziałach oraz krawędzi sieci dostępowych, które są najczęściej obieranymi celami ataków cyberprzestępców.

Podejście Cisco ukierunkowane na wykrywanie i eliminację zagrożeń idealnie spełnia te wymagania. Rozwiązania Cisco przekształcają sieć w mechanizm wykrywający i zabezpieczający, który może szybko wykryć zagrożenia po śladach anomalii ruchu sieciowego i odizolować je, zanim rozprzestrzenią się do innych miejsc w sieci i dokonają większych zniszczeń.

Wraz z wdrożeniem swojej nowoczesnej architektury oprogramowania Cisco ONE, Cisco upraszcza też proces zakupu funkcji zabezpieczeń dla centrów danych, oddziałów i krawędzi sieci dostępowych. Klienci, którzy zakupią pakiet zabezpieczeń oprogramowania Cisco ONE, otrzymają następujące korzyści:

Przyjazne w obsłudze i wszechstronne pakiety oprogramowania dostosowane do konkretnej domeny

Możliwość rozpoczęcia wdrożenia w dowolnym miejscu

Dostęp do najnowszych informacji o zagrożeniach i funkcji
Oferty abonamentowe zapewniające przewidywalność inwestycji

Oprogramowanie Cisco ONE ułatwia zabezpieczenie sieci; dzięki nowemu rozwiązaniu Cisco klienci mogą dobrać odpowiedni pakiet do swoich obecnych potrzeb, a jednocześnie zyskują możliwość ochrony inwestycji w przyszłości. Tym właśnie różni się oferta Cisco od oferty wielu innych dostawców – Cisco ONE pozwala zabezpieczyć więcej miejsc w sieci i zapewnia bardziej rozbudowaną ochronę.

Migracja na model oprogramowania Cisco ONE to priorytet dla każdej firmy, która chce usprawnić swoją strategię bezpieczeństwa. Firma ZK Research przygotowała następujące zalecenia:

Era cyfrowa to czas na nowe podejście do zabezpieczeń. Tradycyjne metody zabezpieczeń zostały stworzone w czasach, gdy dział IT miał ścisłą kontrolę nad aplikacjami, punktami końcowymi oraz miejscem pracy użytkowników. Te czasy minęły, a działy IT utraciły kontrolę, którą niegdyś miały. Firmy muszą przyjąć podejście ukierunkowane na wykrywanie i usuwanie zagrożeń, które wykorzystuje sieć – integralny zasób przedsiębiorstwa – i pozwala na monitorowanie całego ruchu oraz szybką identyfikację naruszeń zabezpieczeń.

Warto zminimalizować liczbę dostawców zabezpieczeń. Według wyników badania 2016 Security Survery przeprowadzonego przez ZK Research, przeciętne środowisko informatyczne firm wykorzystuje produkty pochodzące od 32 dostawców zabezpieczeń. Praca z tak dużą liczbą dostawców skutkuje powstaniem środowiska, którym trudno zarządzać. Takie środowisko jest pełne martwych punktów, fałszywych pozytywów oraz niespójnych informacji. Celem firmy powinno być zmniejszenie liczby dostawców zabezpieczeń celem usprawnienia wydajności i uproszczenia procesów obsługi. Najprawdopodobniej nie da się uniknąć stosowania produktów wielu dostawców, ale warto wybrać głównego dostawcę z dużym ekosystemem produktów podmiotów zewnętrznych, które zapewnią spójność współpracy.

Klientom zainteresowanym zwiększeniem swojego zabezpieczenia polecamy oprogramowanie Cisco ONE. W tym dokumencie opisano, dlaczego oprogramowanie Cisco ONE jest korzystniejsze pod względem innowacyjności oraz kosztów od tradycyjnych modeli zakupowych. Według wniosków ZK Research, oprogramowanie Cisco ONE Software to odpowiedni model zakupu zabezpieczeń dla centrów danych, sieci WAN oraz sieci dostępowych dla biznesu w erze cyfrowej.

KONTAKT

zeus@zkresearch.com

Tel. kom.: 301-775-7447
Tel. biurowy: 978-252-5314