

OPRACOWANIE

Dostęp do sieci na zasadzie zerowego zaufania powinien być powszechny

Dlaczego strategia zerowego zaufania oparta na zaporze ma sens w przypadku sieci hybrydowych?



Streszczenie

Wzrost popularności pracy zdalnej sprawił, że w centrum uwagi pojawiła się koncepcja dostępu do sieci na zasadzie zerowego zaufania (ZTNA). Do powstania tej koncepcji doprowadziło wyczerpanie się możliwości działania dotychczasowego modelu zabezpieczeń sieci stosowanego w wirtualnych sieciach prywatnych (VPN), zgodnie z którym to, co znajduje się wewnątrz sieci, jest godne zaufania, a to, co znajduje się na zewnątrz sieci, godne zaufania nie jest.

W modelu ZTNA, użytkownicy lub urządzenia żądające dostępu do określonych zasobów muszą najpierw przejść weryfikację, zanim uzyskają taki dostęp. Często zakłada się, że koncepcja ZTNA znajduje zastosowanie tylko w chmurze. Założenie to jest jednak nie tylko nieprawdziwe, ale może również prowadzić do poważnych problemów z bezpieczeństwem i zbędnej złożoności. Z wielu powodów większość przedsiębiorstw korzysta z sieci hybrydowych, w przypadku których użytkownicy i urządzenia muszą mieć dostęp do zasobów w dowolnym miejscu, o dowolnej porze i z dowolnego miejsca.

Gdy przedsiębiorstwa wdrażają środowiska hybrydowe, zapory są stale udoskonalane. Uzupełnienie zapory o funkcje ZTNA sprawia, że zapory takie będą odgrywać kluczową rolę w modelu zabezpieczeń sieci, ponieważ przedsiębiorstwa chcą zapobiegać naruszeniom bezpieczeństwa i chronić zasoby zarówno lokalnie, jak i w chmurze.

Zarządzanie środowiskami hybrydowymi zainstalowanymi lokalnie i w chmurze

Wzrost liczby operacji chmurowych dotyczących wszystkich elementów systemu, od infrastruktury po oprogramowanie, zapewnia elastyczność i sprawność działania. Obecnie coraz więcej użytkowników potrzebuje dostępu do aplikacji chmurowych służących do przechowywania, przesyłania i przetwarzania informacji wrażliwych. Nic więc dziwnego, że aplikacje te stały się celem dla cyberprzestępców. Zabezpieczenia wdrożone w chmurze w celu ochrony aplikacji i infrastruktury chmury muszą być zatem zdolne do współdzielenia i korelowania informacji o zagrożeniach, aby zapewnić szeroką widoczność sieci i zapobiegać rozprzestrzenianiu się złośliwego oprogramowania. Wszystkie elementy sieci muszą być odpowiednio zabezpieczone za pomocą spójnych zasad i kontroli we wszystkich środowiskach operacyjnych, zwłaszcza obejmujących wiele chmur.

Przejście do aplikacji chmurowych niewątpliwie następuje, ale bezpieczeństwo lokalne również jest ważne. Czy to ze względów biznesowych, czy też z uwagi na zgodność z przepisami, kwestie kontroli, koszty, dostępność lub bezpieczeństwo, wiele przedsiębiorstw nie korzysta wyłącznie z rozwiązań chmurowych. Są nawet takie, w których funkcjonuje jedynie tradycyjne centrum danych. Niektórzy specjaliści twierdzą, że sieci lokalne są już martwe, ale w rzeczywistości nową normą stają się sieci hybrydowe obejmujące zarówno środowiska lokalne, jak i chmurowe. Chmura jest dobrym rozwiązaniem do obsługi obciążeń elastycznych, nieprzewidywalnych, infrastruktura lokalna sprawdza się natomiast w przypadku obciążeń stabilnych i oferuje przy tym niższy całkowity koszt posiadania. Niektóre przedsiębiorstwa przeszły nawet na rozwiązania chmurowe w odniesieniu do niektórych aplikacji, a następnie powróciły do infrastruktury lokalnej.

Oparcie się na aplikacjach jako centralnym filarze nowoczesnego przedsiębiorstwa oraz szybkie przyjęcie i integracja Internetu rzeczy (IoT) oznacza, że sieci ewoluują. Ponadto z uwagi na fakt, że zbiory big data, architektury hiperskalowalne, rozwiązania SD-WAN, sieci 5G oraz systemy inteligentne stosowane w samochodach, miastach i infrastrukturze stają się powszechne, ewolucja ta będzie musiała postępować dalej. Korzyści płynące z lokalnego przetwarzania danych na potrzeby tych aplikacji powodują odejście od przetwarzania w chmurze do przetwarzania na brzegu sieci w pobliżu źródła danych (edge computing). Niezależnie od rodzaju zastosowanego urządzenia brzegowego, musi być ono zdolne do nawiązania bezpiecznego połączenia z innym urządzeniem brzegowym lub zbiorem urządzeń brzegowych w dowolnym czasie i z dowolnego miejsca.

Warto upraszczać

W środowiskach hybrydowych złożoność sieci może stanowić szczególny problem, a zabezpieczenia i funkcje sieciowe muszą być zintegrowane. Próba zarządzania wszystkimi alertami, fałszywymi alarmami i sprzecznymi zasadami w różnych produktach punktowych nieuchronnie prowadzi do powstania luk zabezpieczeniowych i zwiększenia podatności na ataki. Jeśli systemy zabezpieczeń działają niezależnie od sieci, analiza i interpretacja pochodzących z nich danych może być czasochłonna. Tymczasem zanim zagrożenie zostanie wykryte, szkody są już często wyrządzone.

Złożoność sieci wynika częściowo z tego, że dawniej tradycyjne funkcje sieciowe i zabezpieczenia były od siebie oddzielone. Funkcje sieciowe obejmowały routery, koncentratory VPN, przełączniki i bezprzewodowe punkty dostępowe, natomiast w skład zabezpieczeń wchodziły zapory, programy antywirusowe, systemy zapobiegania włamaniom, zabezpieczenia DNS i piaskownice. W skład środków bezpieczeństwa wchodziły zapory, programy antywirusowe, systemy zapobiegania włamaniom, mechanizmy filtrowania stron WWW i treści, zabezpieczenia DNS i bezpieczne środowiska testowe (sandbox).



Liczba naruszeń bezpieczeństwa danych rośnie, a ponieważ przedsiębiorstwa przenoszą coraz więcej swoich funkcji biznesowych do chmury, ataki na aplikacje WWW stanowią obecnie 39% wszystkich takich naruszeń¹.

W skład funkcji sieciowych i zabezpieczeń wchodziły natomiast różne produkty punktowe, którymi nie dało się zarządzać z poziomu jednego urządzenia, ponieważ żadne urządzenie nie dysponowało wystarczającą mocą obliczeniową zdolną do łącznej obsługi i analizy tych funkcji sieciowych i zabezpieczeń. Ponadto przedsiębiorstwa zbyt często wyłączały w swoich zaporach zabezpieczenia i funkcje deszyfrowania ze względu na ich negatywny wpływ na wydajność.

Luki w funkcjach sieciowych mogą skutkować mniejszą wydajnością, ale nie mają charakteru krytycznego. Luka w zabezpieczeniach może natomiast prowadzić do poważnego incydentu związanego z bezpieczeństwem. Przedsiębiorstwa muszą zatem rozważyć zalety i wady wdrażania i integrowania różnych zasad, konfiguracji i systemów operacyjnych oraz zarządzania nimi.

Stosowane przez cyberprzestępców metody ataków są zorganizowane, elastycznie dostosowują się do sytuacji i przewidują wymianę informacji, podczas gdy zabezpieczenia zainstalowane w większości sieci do takich działań nie są zdolne. Ponadto wspomniane metody są specjalnie ukierunkowane na omijanie i wykorzystywanie słabych punktów architektury zabezpieczeń.

Aby zmniejszyć złożoność i poprawić skuteczność zabezpieczeń, warto zatem szukać produktów zintegrowanych. Osoby zarządzające siecią potrzebują bowiem większej zgodności pomiędzy różnymi zabezpieczeniami wdrożonymi w przedsiębiorstwie, a same te zabezpieczenia powinny być zdolne do wymieniać się informacjami o zagrożeniach w czasie rzeczywistym oraz zapewnienia stabilnego, wysokiego poziomu wydajności sieci. Aby zwiększyć interoperacyjność z istniejącymi i przyszłymi rozwiązaniami, zabezpieczenia te powinny również działać w oparciu o otwarte standardy.

Przed wszystkim zapora

Zapory są centralnym elementem tego typu spójnej, zintegrowanej strategii zabezpieczeń. Nie są to w żadnym razie urządzenia statyczne i od lat nieustannie dodawane są do nich nowe funkcje. Poniżej przedstawiono krótki opis zmian, jakim podlegały zapory na przestrzeni lat.

- **Filtry pakietów i translacja adresów sieciowych.** Filtrowanie pakietów i translacja adresów sieciowych (NAT) to funkcje służące do monitorowania i kontrolowania pakietów przechodzących przez interfejs sieciowy, stosowania określonych reguł bezpieczeństwa oraz izolowania sieci wewnętrznej od publicznego Internetu.
- **Kontrola stanowa.** Funkcja dynamicznego filtrowania pakietów monitoruje stan połączeń i określa rodzaje pakietów danych należących do znanego, aktywnego połączenia, które mogą być przepuszczane przez zaporę.
- **Ujednolicone zarządzanie zagrożeniami (UTM).** Urządzenia UTM oferowały w jednym urządzeniu (zwykle z ujednoliconą konsolą do zarządzania) wiele z najważniejszych funkcji zabezpieczeń, w tym zaporę, system zapobiegania włamaniom, koncentrator VPN, bramę antywirusową oraz mechanizmy filtrowania treści i równoważenia obciążenia w sieci rozległej.
- **Zapora następnej generacji (NGFW).** To urządzenie zabezpieczające typu „wszystko w jednym” jest oparte na modelu UTM, ale oferuje przy tym skalowalność i wydajność klasy korporacyjnej oraz pozwala na szczegółową inspekcję ruchu w warstwie aplikacji (warstwa 7).

Zapory NGFW zostały wzbogacone o funkcje ułatwiające segmentację wewnętrzną, możliwość integracji z bezpiecznym środowiskiem testowym, mechanizmy inspekcji SSL, rozwiązanie SD-WAN, a ostatnio także funkcje ZTNA. Mechanizmy przetwarzania danych na brzegu sieci korzystają z zainstalowanych lokalnie zapor, w przypadku których dane są również przetwarzane lokalnie. Rozwiązania takie są bardziej energooszczędne niż maszyny wirtualne, a także charakteryzują się mniejszymi opóźnieniami, ponieważ odpada element przesyłania danych do chmury i z powrotem.

Utworzenie centralnego punktu zapewniającego odpowiednią widoczność i kontrolę

Jeśli zapora NGFW jest podstawą funkcji sieciowych i zabezpieczeń, może ona pełnić rolę centralnego punktu zapewniającego odpowiednią widoczność i kontrolę, o ile tylko jest zdolna do wykrywania i kontrolowania danych do niej przesyłanych. Jeśli zapora NGFW współdzieli bazowe połączenie ze zintegrowanymi produktami, cały mechanizm kontroli może zostać odpowiednio skonsolidowany. Zarówno funkcje sieciowe, jak i zabezpieczenia mogą być konfigurowane i kontrolowane, co eliminuje potrzebę przemieszczania się pomiędzy produktami punktowymi. Stosowane zasady mogą być łączone w centralnym punkcie kontrolnym, a następnie zarządzane za pomocą jednej konsoli, co przyspiesza pracę i zmniejsza ryzyko popełnienia błędu przez człowieka.



Średni globalny koszt naruszenia bezpieczeństwa danych wynosi 3,86 mln USD, a trzy najczęstsze wektory ataku to przejęcie danych uwierzytelniających (19%), wykorzystanie błędnej konfiguracji chmury (19%) oraz wykorzystanie luk w zabezpieczeniach oprogramowania innych firm (16%)².

Tego typu centralizacja wpływa również na dzienniki i raporty. W przypadku używania produktów punktowych dane muszą być agregowane i oczyszczane ręcznie lub za pomocą innego produktu punktowego. Jeśli jednak wszystko jest podłączone do zapory, agregacja funkcji zapewnienia widoczności, rejestrowania i raportowania może znacznie ułatwić przeprowadzanie audytów zgodności z przepisami. Ponadto można automatycznie generować lub dostosowywać raporty w celu przedstawiania informacji na czytelnych wizualizacjach.

Dodanie do zainstalowanych lokalnie zabezpieczeń funkcji dostępu do sieci na zasadzie zerowego zaufania

Dodanie do zapór funkcji dostępu do sieci na zasadzie zerowego zaufania (ZTNA) to wielki krok do przodu w dziedzinie zdalnego dostępu i zabezpieczeń lokalnych. Ze względu na to, że użytkownicy uzyskują dostęp do zasobów spoza tradycyjnej sieci, a sieci takie mają wiele brzegów, zaufanie nie może już zależeć od lokalizacji użytkownika. W kontekście pracy zdalnej, konieczne jest zastosowanie do zdalnego dostępu zasady zerowego zaufania, co powoduje rozszerzenie modelu zerowego zaufania poza sieć. W przeciwieństwie do wirtualnej sieci prywatnej (VPN), która skupia się wyłącznie na kwestiach sieciowych, model dostępu do sieci na zasadzie zerowego zaufania idzie o warstwę w górę, efektywnie zabezpieczając aplikacje niezależnie od sieci. Ponadto model ZTNA:

- zapewnia większą użyteczność niż sieć VPN;
- zwiększa bezpieczeństwo dzięki funkcjom bieżącej weryfikacji i szczegółowego nadzoru nad dostępem do aplikacji;
- kontroluje dostęp do aplikacji bez względu na ich lokalizację (lokalnie, w chmurze prywatnej lub w chmurze publicznej);
- w pełni obsługuje hybrydowe modele sieci oraz zapewnia bezpieczeństwo zarówno użytkownikom stacjonarnym, jak i zdalnym.

Powszechnie uważa się, że funkcja ZTNA jest dostępna tylko w chmurze lub stanowi część rozwiązań SASE, jest to jednak błędny pogląd, który wynika z faktu, że wielu dostawców nie oferuje korzyści płynących ze skonsolidowanych zabezpieczeń zapory NGFW. Funkcja ta jednak jeszcze lepiej sprawdza się w zaporach zainstalowanych lokalnie, zaporach maszyn wirtualnych i rozwiązaniach SASE. Oparta na zaporze elastyczna implementacja funkcji ZTNA jest idealna dla współczesnych środowisk hybrydowych, ponieważ oferuje spójne zasady dla rozwiązań zainstalowanych lokalnie oraz chmur prywatnych i publicznych.

Podsumowanie

Z biegiem czasu funkcja ZTNA stanie się standardowym elementem każdego kompleksowego systemu zabezpieczeń i ze względu na swoje zalety w zakresie bezpieczeństwa i łatwości użycia zastąpi większość (jeśli nie wszystkie) opartych na użytkownikach systemów zdalnego dostępu do sieci VPN. W przeciwieństwie do wieloetapowego procesu w przypadku sieci VPN, nawiązanie bezpiecznego połączenia z funkcją ZTNA jest bezproblemowe. Wystarczy kliknąć ikonę aplikacji, aby natychmiast uzyskać bezpieczne połączenie. Jako że podejście ZTNA rozszerza model zerowego zaufania poza sieć, zmniejsza tym samym powierzchnię ataku, izolując aplikacje od Internetu.

W miarę jak coraz więcej przedsiębiorstw wdraża podejście ZTNA, jedynym zastosowaniem sieci VPN będzie obsługa połączeń typu „site-to-site” i „machine-to-machine”. Potrzeba łączenia zdalnych użytkowników i urządzeń z dowolnego miejsca nie zniknie. Dzięki wdrożeniu zaawansowanej strategii zerowego zaufania opartej na zaporze można jednak lepiej zabezpieczać dane klientów, chronić i kontrolować dostęp do krytycznych zasobów oraz zmniejszyć złożoność zabezpieczeń.

Zapory to istotny element systemu zabezpieczeń zarówno obecnie, jak i w przyszłości. Nadal będą one odgrywać kluczową rolę w ochronie użytkowników i aplikacji zarówno lokalnie, jak i w chmurze.

¹ „[2021 Data Breach Investigations Report](#)”, Verizon, maj 2021 r.

² „[2020 Cost of a Data Breach Report](#)”, IBM Security, lipiec 2020 r.