PUNKT WIDZENIA

Poza VPN

Uniwersalne podejście ZTNA przyszłością bezpiecznego zdalnego dostępu

Streszczenie

We współczesnym coraz bardziej połączonym świecie zdalny dostęp nie jest już dla wielu organizacji luksusem, ale koniecznością. W celu zapewnienia bezpiecznego zdalnego dostępu zaczęto więc powszechnie korzystać z wirtualnych sieci prywatnych (VPN). Chociaż sieci te są bezpieczne, cechują je pewne ograniczenia architektury, które uniemożliwiają zaspokojenie bieżących potrzeb w zakresie bezpieczeństwa. Lepszym rozwiązaniem okazuje się obecnie zdalny dostęp na zasadzie zerowego zaufania („zero-trust network access", ZTNA) — podejście, które umożliwia bardziej bezpieczne, skalowalne i przyjazne dla użytkownika korzystanie ze zdalnego dostępu.

Zagrożenia związane z przemieszczaniem się złośliwego oprogramowania i oprogramowania ransomware między zasobami w sieci wewnętrznej

Cyberataki nie są żadnym nowym zagrożeniem, ale coraz większe obawy specjalistów ds. bezpieczeństwa sieci budzą próby przemieszczania się zagrożeń w sieci wewnętrznej po jej zainfekowaniu. Taki ruch boczny („lateral movement") oznacza grupę wykorzystywanych przez cyberprzestępców metod eksploracji zainfekowanej sieci w celu znalezienia podatności, eskalacji uprawnień dostępu i realizacji zamierzeń. Słowo „boczny" określa sposób, w jaki haker przemieszcza się między urządzeniami, aplikacjami itp.

Chociaż sieci VPN zapewniają bezpieczne połączenie, ich architektura nie zapobiega bocznemu przemieszczaniu się złośliwego oprogramowania. Ryzyko związane z takim bocznym przemieszczaniem się złośliwego oprogramowania staje się jeszcze istotniejsze w kontekście pracowników hybrydowych, którzy pracując zdalnie z dowolnego miejsca płynnie „przełączają się" między pracą zdalną a pracą stacjonarną.

Ewolucja podejścia ZTNA

Uniwersalne podejście ZTNA, będące zaawansowanym etapem rozwoju podejścia ZTNA, wychodzi naprzeciw wspomnianym wyzwaniom. Na bazie zasady „nigdy nie ufaj, zawsze sprawdzaj" stale bowiem uwierzytelnia użytkowników i urządzenia oraz przyznaje dostęp tylko do konkretnych aplikacji lub zasobów, które są w danym momencie potrzebne. Taki oparty na najmniejszych uprawnieniach model znacznie zmniejsza powierzchnię ataku i minimalizuje potencjalny wpływ naruszeń. Ponadto podejście ZTNA korzysta z dynamicznych mechanizmów kontroli dostępu, stale weryfikując tożsamość użytkownika i stan urządzenia przed ewentualnym przyznaniem mu dostępu. W ten sposób tylko autoryzowani i sprawdzeni użytkownicy mogą uzyskać dostęp do danych wrażliwych, a w przypadku wykrycia naruszenia, dostęp ten może im zostać odebrany w czasie rzeczywistym.

Oprócz poprawy bezpieczeństwa, uniwersalne podejście ZTNA oferuje kilka innych korzyści w porównaniu z sieciami VPN. Podejście to jest z natury skalowalne i może obsługiwać zmieniającą się liczbę użytkowników zdalnych bez wpływu na wydajność. To czyni je idealnym rozwiązaniem dla organizacji z dynamicznie rosnącą liczbą pracowników lub z sezonowymi wzrostami zapotrzebowania na zdalny dostęp.

Płynniejsze i efektywniejsze działanie

Z perspektywy użytkownika uniwersalne podejście ZTNA oferuje bardziej płynne i efektywne środowisko. Eliminuje potrzebę ręcznej konfiguracji sieci VPN, zapewniając użytkownikom szybki i łatwy dostęp do aplikacji z dowolnego urządzenia. Ponadto nie wymaga przesyłania całego ruchu sieciowego przez centralny serwer VPN, co może znacznie poprawić wydajność, zwłaszcza w przypadku użytkowników rozproszonych geograficznie.

Chociaż uniwersalne podejście ZTNA oferuje znaczne korzyści w porównaniu z sieciami VPN, należy pamiętać, że nie jest to rozwiązanie idealne. Niektóre potencjalne wyzwania obejmują tu potrzebę integracji z istniejącą infrastrukturą bezpieczeństwa oraz możliwość wystąpienia wąskich gardeł wydajności i opóźnień ruchu, w przypadku nieprawidłowego wdrożenia tego podejścia. Przy starannym planowaniu i wykonaniu, wyzwaniom tym można jednak łatwo sprostać.

Podsumowanie

Uniwersalne podejście ZTNA to istotny krok naprzód w dziedzinie zapewniania bezpiecznego dostępu zdalnego. Eliminując model wbudowanego zaufania VPN i przyjmując zasadę najmniejszych uprawnień, uniwersalne podejście ZTNA rozwiązuje krytyczne obawy związane z bezpieczeństwem. Jednocześnie oferuje lepszą skalowalność, lepsze wrażenia użytkownika i większą efektywność operacyjną. Ponadto wspomniane pryncypia bezpieczeństwa w zakresie dostępu zdalnego można zastosować do zabezpieczenia dostępu do sieci wewnętrznej w ramach uniwersalnego podejścia ZTNA, obniżając ryzyko związane z nowym hybrydowym modelem pracy.

Jako że świat nadal podąża w kierunku bardziej zdalnego środowiska pracy, uniwersalne podejście ZTNA jest bez wątpienia przyszłością bezpiecznego zdalnego dostępu. Organizacje, dla których priorytetem jest bezpieczeństwo, elastyczność i wrażenia użytkownika, powinny poważnie rozważyć przejście z modelu VPN na uniwersalne podejście ZTNA, aby zapewnić swoim pracownikom zdalnym solidne i zgodne z przyszłymi standardami rozwiązanie.

5 listopada 2024 10:17 AM

2481925-A-0-PL