OPRACOWANIE

SASE jako mechanizm zapewnienia cyberbezpieczeństwa dla pracowników hybrydowych

Nowatorskie podejście do ochrony użytkowników, urządzeń, lokalizacji i aplikacji

Streszczenie

Organizacje muszą stale wspierać i zabezpieczać swoich pracowników zdalnych. Praca coraz częściej wymaga dostępu do zasobów sieciowych z różnych lokalizacji i urządzeń. Jest to niezwykle ważne, ponieważ zdalny dostęp do sieci wprowadza nowe wektory ataku zwiększając podatności na zagrożenia. Wymaga to wdrożania skutecznych zabezpieczeń chroniących przed stale rozwijającymi się cyberzagrożeniami.

Rosnąca popularność pracy zdalnej i ekspansja zagrożeń cyfrowych wymagają kompleksowego podejścia do kwestii bezpieczeństwa i sprostania takim wyzwaniom, jak spójne egzekwowanie zasad bezpieczeństwa, zapewnienie płynnego dostępu do zasobów w chmurze i scentralizowanie zarządzania. Architektura SASE (Secure Access Service Edge) oferuje nowatorskie podejście do integracji mechanizmów zapewnienia cyberbezpieczeństwa pracownikom hybrydowym polegające na połączeniu funkcji sieciowych z funkcjami bezpieczeństwa oferowanych formie usługi w ramach natywnej platformy chmurowej. Architektura SASE chroni użytkowników, urządzenia, lokalizacje i aplikacje, niezależnie od ich środowiska sieciowego.

73% przedstawicieli ścisłej kadry kierowniczej uważa, że pracownicy zdalni stanowią większe zagrożenie dla bezpieczeństwa[1].

Architektura SASE wykracza poza tradycyjne rozwiązania sieciowe i zabezpieczające, integrując funkcje chmurowych usług zabezpieczających (SSE), lokalne rozwiązanie SD-WAN, usługi bezpieczeństwa, dostęp na zasadzie zerowego zaufania oraz scentralizowane funkcje zarządzania i monitorowania jakości pracy użytkowników. To kompleksowe podejście pozwala organizacjom na poprawę stanu bezpieczeństwa, zwiększenie wydajności operacyjnej oraz wsparcie bezpiecznego i produktywnego środowiska pracy dla każdego pracownika niezależnie od jego lokalizacji lub urządzenia z którego korzysta. SASE to przyszłościowa architektura bezpieczeństwa pracy hybrydowej, zachęcająca organizacje do korzystania z możliwości, jakie niesie ze sobą praca zdalna, przy jednoczesnym efektywnym ograniczaniu związanego z nią ryzyka.

Sposób na uproszczenie dostarczania cyberbezpieczeństwa dla pracowników hybrydowych

Wraz ze wzrostem liczby pracowników hybrydowych organizacje muszą zabezpieczać ich dostęp do sieci i aplikacji zarówno wtedy, gdy pracują stacjonarnie, jak i wtedy, gdy pracują zdalnie. Upowszechnienie się modelów pracy zdalnej znacznie rozszerzyło powierzchnię ataku na biura domowe i lokalizacje zdalne, zwiększając tym samym złożoność systemów ochrony sieci, aplikacji i zasobów.

Mając do czynienia z wieloma takimi odległymi lokalizacjami i pracownikami zdalnymi, organizacje często napotykają trudności w spójnym stosowaniu i egzekwowaniu zasad bezpieczeństwa oraz zapewnieniu optymalnego środowiska pracy dla wszystkich swoich pracowników hybrydowych. Wyjątkowym wyzwaniem jest teraz zabezpieczenie takiego środowiska, ponieważ jego ewolucja następowała w sposób organiczny, a nie w ramach starannie opracowanej strategii.

Dynamiczne mnożenie się nowych punktów dostępu do sieci i podłączanie do niej urządzeń kolejnych pracowników zdalnych, często wdrażane w ramach niezależnych projektów, doprowadziło do pojawienia się różnych podatności chętnie wykorzystywanych przez cyberprzestępców. Ponadto trend ten skutkuje również ograniczoną widocznością działania użytkowników, urządzeń i aplikacji, co skutkuje większą liczbą zagrożeń i luk w zabezpieczeniach.

Architektura SASE pomaga sprostać tym wyzwaniom, zapewniając bezpieczny dostęp i wydajne możliwości połączenia dla użytkowników w dużych i małych oddziałach oraz odległych lokalizacjach. Wiele rozwiązań SASE rozwiązuje jednak tylko część problemu. Nie zapewniają one pracownikom hybrydowym spójnego modelu cyberbezpieczeństwa klasy korporacyjnej lub nie są zdolne do płynnej integracji z różnymi fizycznymi i wirtualnymi narzędziami sieciowymi i zabezpieczającymi wdrożonymi w punktach dostępu do sieci. W rezultacie nie potrafią zapewnienić użytkownikom spójnego poziomu cyberbezpieczeństwa lub zagwarantować odpowiedniej jakości pracy.

Zintegrowane rozwiązanie SASE do zabezpieczania użytkowników, urządzeń i lokalizacji

Architektura SASE to nowatorskie podejście do bezpieczeństwa sieci, polegające na ujednoliceniu różnych funkcji sieciowych i zabezpieczających w ramach jednej, natywnej dla chmury platformy. Jednym z podstawowych założeń architektury SASE jest jej zdolność do zabezpieczania użytkowników, lokalizacji i aplikacji niezależnie od ich lokalizacji lub środowiska sieciowego.

Zabezpieczenie użytkowników i lokalizacji

Architektura SASE zapewnia, że użytkownicy, niezależnie od tego, czy pracują stacjonarnie, czy zdalnie, są w spójny sposób chronieni przed zagrożeniami. Architektura SASE zapewnia wspomnianą ochronę we wszystkich lokalizacjach, w których użytkownicy uzyskują dostęp do zasobów sieciowych, w tym w oddziałach firmy lub w lokalizacjach takich jak poczekalnia na lotnisku lub kawiarnia na mieście.

Zabezpieczenie dostępu do aplikacji

Obecnie aplikacje znajdują się w różnych środowiskach, w tym w centrach przetwarzania danych, chmurach publicznych lub na platformach SaaS (Software-as-a-Service). Architektura SASE zapewnia, że wszyscy użytkownicy, którzy uzyskują dostęp do takich aplikacji, niezależnie od ich środowiska hostingowego, są chronieni przed cyberzagrożeniami i naruszeniami ochrony danych. Dzięki integracji takich funkcji jak broker zabezpieczeń dostępu do chmury (CASB), dostęp do sieci na zasadzie zerowego zaufania (ZTNA) oraz oferowane przez rozwiązanie SD-WAN inteligentne mechanizmy routingu i sterowania ruchem, architektura SASE zapewnia kompleksową ochronę zarówno dla aplikacji SaaS, jak i starszych aplikacji.

Zintegrowana platforma zabezpieczeń

Centralnym elementem architektury SASE jest zintegrowana platforma zabezpieczeń, która płynnie łączy różne usługi bezpieczeństwa, w tym między innymi zaporę następnej generacji (Next Generation Firewall, NGFW), bezpieczną bramę internetową (Secure Web Gateway, SWG), model ZTNA i bezpieczne rozwiązanie SD-WAN. Dzięki takiemu zintegrowanemu podejściu organizacje mogą ujednolicić swoje reguły bezpieczeństwa, zmniejszyć liczbę agentów, uprościć procesy wdrażania i zarządzania komponentami, a także ograniczyć powierzchnię ataku poprzez wyeliminowanie silosów bezpieczeństwa i martwych punktów.

Przejście na pracę zdalną wiąże się niestety z ogromnym wzrostem zagrożeń dla cyberbezpieczeństwa. Zagrożenia te obejmują phishing, smishing i oprogramowanie wymuszające okup (ransomware). Średni koszt naruszenia ochrony danych w organizacjach zatrudniających do 500 pracowników wynosi 3,31 mln USD, a całkowity koszt takich naruszeń nigdy nie jest od razu znany[2].

Skalowalność i elastyczność

Architektura SASE zapewnia elastyczność i skalowalność, aby na bieżąco uwzględniać zmieniające się potrzeby nowoczesnych organizacji, w tym obsługiwać zarówno małe oddziały, jak i globalnie rozproszonych pracowników. W ten sposób organizacje utrzymują spójny stan bezpieczeństwa niezależnie od swojej wielkości, branży lub zasięgu geograficznego.

Poprawa jakości pracy użytkowników

Bezpieczne rozwiązanie SD-WAN usprawnia łączność, operacje i dostęp do aplikacji poprzez rozszerzenie i zabezpieczenie lokalnej sieci WAN. Wszystkie te elementy bardzo pozytywnie wpływają na doświadczenia użytkowników hybrydowych. Po integracji bezpiecznego rozwiązania SD-WAN z komponentami SSE, ruch danych z i do aplikacji jest inteligentnie i dynamicznie przekierowywany przez odpowiednie łącza, zapewniając użytkownikom stacjonarnym i zdalnym wysoką produktywność oraz bezpieczny i wydajny dostęp do aplikacji korporacyjnych.

Kluczowe komponenty architektury SASE

Chociaż większość rozwiązań sieciowych rozwijano wystarczająco szybko, aby wspierać przepływy pracy użytkowników zdalnych, biur i punktów końcowych, rozwój większości narzędzi i rozwiązań zabezpieczających nie nadążał za tymi zmianami. Brak było zatem spójnych zabezpieczeń i rozwiązań zapewniających optymalne doświadczenia użytkownikom zdalnym i stacjonarnym.

W dzisiejszym kontekście pracy zdalnej, w którym pracownicy wymagają bezpiecznego dostępu do aplikacji z różnych lokalizacji i urządzeń, sieci VPN nie zapewniają niezbędnego poziomu bezpieczeństwa i elastyczności. Architektura SASE stała się nowoczesnym rozwiązaniem w zakresie zabezpieczania zdalnego dostępu i pracy hybrydowej, oferując kompleksowe podejście do bezpieczeństwa.

Wydajne rozwiązanie SASE łączy wiele funkcji bezpieczeństwa, w tym NGFW, SWG, ZTNA, CASB, funkcje zdalnej izolacji przeglądarek (Remote Browser Isolation, RBI), ochrony przed utratą danych (Data Loss Prevention, DLP) i kompleksowego monitorowania środowiska cyfrowego (Digital Experience Monitoring, DEM) oraz rozwiązanie SD-WAN, w jedną, zintegrowaną platformę. Ta zintegrowana architektura natywna dla chmury pozwala organizacjom skonsolidować stos zabezpieczeń, uprościć zarządzanie, poprawić jakość pracy zdalnej, zapewnić spójne zabezpieczenia i poprawić widoczność całej infrastruktury sieciowej. Ponadto oferuje bezpieczny dostęp do aplikacji korporacyjnych, aplikacji SaaS i Internetu, zapewniając pełną ochronę przed wszelkiego typu zagrożeniami.

Architektura SASE musi również obejmować model bezpieczeństwa oparty na zerowym zaufaniu, z pojedynczym i ujednolicony agentem, gdzie dostęp do zasobów sieciowych opiera się na rygorystycznych mechanizmach uwierzytelniania, autoryzacji i ciągłej weryfikacji. W ramach takiego modelu organizacje mogą ograniczyć ryzyko ataku ze strony osób z wewnątrz, nieautoryzowanego dostępu oraz rozprzestrzeniania się zagrożeń w sieci wewnętrznej.

Rozwiązania SASE wykorzystują kompleksowe, oparte na sztucznej inteligencji źródła informacji o zagrożeniach i narzędzia analityczne służące do identyfikacji i neutralizacji zaawansowanych zagrożeń w czasie rzeczywistym. Dzięki wykorzystaniu mechanizmów uczenia maszynowego, analizy behawioralnej i wymiany informacji o zagrożeniach organizacje mogą proaktywnie bronić się przed szeroką gamą cyberzagrożeń, w tym złośliwym oprogramowaniem, oprogramowaniem ransomware, phishingiem i atakami typu zero-day.

Dostawcy architektury SASE powinni wspierać klientów w jej wdrażaniu i dostosowywać ją do zgłaszanych potrzeb. Architektura SASE musi zabezpieczyć wszystkich użytkowników w organizacji (od dużych oddziałów korzystających z technologii SD-WAN, przez mniejsze lokalizacje z łączami LAN, aż po odległe lokalizacje na całym świecie), aby zapewnić im spójne doświadczenia i bezpieczeństwo.

Podsumowanie

Architektura SASE nie ogranicza się jedynie do rozwiązywania bezpośrednich problemów związanych z bezpieczeństwem pracowników hybrydowych, ale zapewnia również skalowalność, elastyczność i sprawność niezbędne, aby dostosować się do zmieniających się potrzeb nowoczesnych przedsiębiorstw. Dzięki konsolidacji zasad bezpieczeństwa, uproszczeniu wdrażania i poprawie widoczności architektura SASE umożliwia działom IT zwiększenie poziomu bezpieczeństwa oraz wsparcie bezpiecznego i produktywnego środowiska pracy.

SASE to przyszłościowa architektura bezpieczeństwa pracy hybrydowej, oferująca przedsiębiorstwom zintegrowaną platformę służącą do zabezpieczenia infrastruktury sieciowej, a także zapewnienia pracownikom możliwości bezpiecznej i produktywnej pracy zdalnej oraz pewnego poruszania się po meandrach epoki cyfrowej.

[1] Kathryn Haan, „Remote Work Statistics and Trends In 2024", Forbes, 12 czerwca 2023 r.

[2] „Zero Trust Security in the Age of Remote Work", i4DM, 23 września 2023 r.

29 lipca 2024 10:02 AM

2589418-0-0-PL