DOSTĘP DO APLIKACJI W PRZEDSIĘBIORSTWIE

Prosty, bezpieczny i pewny

Zapewnienie pracownikom bezpiecznego dostępu do firmowych aplikacji, znajdujących się za zaporą sieciową jest podstawowym wymogiem we wszystkich przedsiębiorstwach. Coraz częściej, firmy muszą radzić sobie z coraz to bardziej ryzykownym rozwiązaniem -zapewnieniem tak samo bezpiecznego dostępu osobom trzecim: kontrahentom, partnerom biznesowym, dostawcom i klientom. Zapewnienie bezpiecznego dostępu do aplikacji, niezależnie od tego, czy jest ono hostowane w chmurze publicznej, czy też w prywatnym centrum danych, jest złożonym i uciążliwym zadaniem wymagającym lokalnego sprzętu i oprogramowania, takiego jak kontrolery dostarczania aplikacji (ADC), wirtualne sieci prywatne (VPN), systemy zarządzania tożsamością (IAM) i inne. A jednak, mimo obecności powyższych technologii, przedsiębiorstwa i tak narażone są na różne zagrożenia bezpieczeństwa, teraz spotęgowane przez rosnącą obecność w sieci niezaufanych użytkowników zewnętrznych. Na szczęście aplikacja skierowana do przedsiębiorstw Akamai Enterprise Application Access rozwiązuje te problemy i pomaga firmom przejść na dostęp zdalny, aby sprostać dzisiejszym wymaganiom mobilnym i tym opartym na chmurze, przy jednoczesnej poprawie ogólnego stanu bezpieczeństwa organizacji.

USŁUGA ENTERPRISE APPLICATION ACCESS

Enterprise Application Access- dostęp do aplikacji firmowych to nowe podejście do zdalnego dostępu. Jest on unikalną, bezpieczną i wygodniejszą alternatywą dla tradycyjnych technologii zdalnego dostępu, takich jak VPN, RDP i proxy. Dzięki Enterprise Application Access nikt nie może dostać się bezpośrednio do aplikacji, ponieważ są one niewidoczne w Internecie i profilu publicznym. Unikalna architektura chmury zamyka wszystkie przychodzące porty zapory, zapewniając jednocześnie uwierzytelnionym użytkownikom końcowym dostęp tylko do określonych aplikacji.Dostęp do aplikacji firmowych Enterprise Application Access integruje ścieżkę ochrony danych, dostęp do tożsamości, bezpieczeństwo aplikacji oraz widoczność zarządzania i kontroli w ramach jednej usługi.

Usługa Enterprise Application Access może zostać wdrożona w zaledwie kilka minut za pośrednictwem ujednoliconego portalu z jednym punktem kontroli, w dowolnym środowisku sieciowym przy niewielkich nakładach finansowych. W rezultacie otrzymujemy bezpieczny model dostępu, który umożliwia zerowy model CapEx, niski OpEx dla krytycznych obciążeń wdrażanych w dowolnym środowisku

DZIAŁANIE

Enterprise Application Access zapewnia bezpieczny dostęp do aplikacji jako usługę, która eliminuje potrzebę stosowania techniki hole-punching w obrębie sieci. Zamiast tego użytkownicy uzyskują dostęp do aplikacji za pośrednictwem chmury, która zatrzymuje

i zabezpiecza dostęp użytkowników daleko poza Twoją siecią. Z Enterprise Application Access nie ma możliwości bezpośredniego dojścia do Twoich aplikacji, pojawia się natomiast bezpieczne, wzajemnie uwierzytelnione połączenie TLS z Twojej sieci lub chmury i doprowadza aplikację do użytkownika.

Ponieważ nie ma tuneli, nie ma opcji żeby złośliwe oprogramowanie znalazło się w obrębie Twojej sieci i potencjalnie rozprzestrzeniło się na wrażliwe lub uprzywilejowane systemy. Wszystkie połączenia użytkowników są zatrzymywane w chmurze i kończą się na bezpiecznych serwerach proxy przy jednoczesnym zastosowaniu silnego uwierzytelniania i kontroli bezpieczeństwa. W razie potrzeby można dodać własne kontrole bezpieczeństwa w celu zwiększenia ochrony najbardziej wrażliwych aplikacji.

Enterprise Application Access umożliwia szybki i intuicyjny dla użytkowników końcowych dostęp do aplikacji. Odchodzą w niepamięć problemy ze słabą wydajnością aplikacji, problemy z łącznością VPN i niekompatybilnością urządzenia. Enterprise Application Access optymalizuje aplikacje i przedstawia je w dowolnej przeglądarce, na dowolnym urządzeniu użytkownika, umożliwiając firmie jednokrotne logowanie i inteligentne wieloczynnikowe uwierzytelnianie. Bezpieczeństwo przestaje być obciążeniem dla użytkowników i pracowników działu IT.

Sieci przedsiębiorstw nie stanowią problemu dla Enterprise Application Access. Dzięki integracji jednym kliknięciem w przypadku Active Directory, dostawców SAML, CDN, serwerów proxy forward, narzędzi SIEM i innych infrastruktur, eliminowane są niestandardowe skrypty oraz integracja. Skalowanie i wdrażanie aplikacji w miejscach publicznych i prywatnych jest bardzo proste dzięki wbudowanym funkcjom wysokiej dostępności, zrównoważonemu obciążeniu serwera i automatycznemu kierowaniu aplikacji.

KORZYŚCI

Wygoda

- Dostęp do aplikacji z dowolnego urządzenie w dowolnej przeglądarce - bez dodatkowego oprogramowania, w tym VPN i wtyczek do przeglądarki
- Wytrzymałe aplikacje i zabezpieczenie potrzeb użytkowników w kilka minut
- Usługa, która konsoliduje ADC, optymalizacja WAN, VPN i 2FA
- Niewymagana wymiana sprzętu ani sieci - reguły zapory, biała lista adresów IP itp.

Bezpieczeństwo

- Wszyscy użytkownicy z dala od Twojej sieci
- Blokada zapory sieciowej lub grupy zabezpieczeń dla całego ruchu przychodzącego
- Twoje aplikacje są niewidoczne w Internecie
- Proste dodawanie MFA do dowolnej aplikacji jednym kliknięciem przycisku

Widoczność

- Kompletna kontrola i raportowanie aktywności użytkownika
- Usługa dostępna jako wbudowane raporty lub zintegrowana z istniejącymi w Twojej firmie narzędziami

DOSTĘP DO APLIKACJI W PRZEDSIĘBIORSTWIE

WZROST NIEZALEŻNYCH PRACOWNIKÓW I RYZYKA Z ICH STRONY - DLACZEGO STANOWIĄ POWAŻNY PROBLEM

Dlaczego ten nowy paradygmat dostępu do aplikacji jest wymagany? Istotne jest, aby w celu zwiększenia produktywności zewnętrzni kontrahenci oraz dostawcy posiadali dostęp do określonych wewnętrznych aplikacji firmy, z którą współpracują. Dzisiaj oznacza to zwykle udzielenie im dostępu do VPN - sieci prywatnej firmy. Jednak jakikolwiek dostęp osób trzecich, tworzy dodatkowe punkty wejścia do sieci organizacji, zwiększając ogólne ryzyko, że krytyczne informacje przedsiębiorstwa - zastrzeżone dokumenty lub dane klientów - mogą wpaść w niepowołane ręce. Niestety nadużycie dostępu przez stronę trzecią jest obecnie znaczącym źródłem naruszeń danych, w tym:

- W ubiegłym roku Trustwave oszacował, że 63% wszystkich naruszeń danych było wynikiem „braku zabezpieczeń u strony trzeciej ”.
- Przeprowadzona w 2014 r. przez CyberArk ankieta dotycząca zagrożeń wykazała, że 60% organizacji zezwala osobom współpracującym z nimi na zdalny dostęp do sieci wewnętrznych.
- W 2013 r. firma McKinsey ogłosiła listę największych banków i firm kredytowych w USA, gdzie średnia liczba dostawców zewnętrznych wynosiła 20 000.
- Według Booz Allen Hamilton osoby trzecie były największym zagrożeniem bezpieczeństwa dla firm sektora finansowego w 2015 roku.
- PwC poinformował, że zewnętrzni dostawcy przyczyniają się do wzrostu liczby incydentów związanych z cyberbezpieczeństwem wśród firm produkcyjnych. W ankiecie z 2014 r. stwierdzono, że liczba tych incydentów wzrosła o 17%, podczas gdy koszt naruszeń skoczył o 38%.

WYZWANIE: ZARZĄDZANIE ZDALNYM DOSTĘPEM DO APLIKACJI JEST BARDZO SKOMPLIKOWANE

Wzrost liczby osób trzecich, pracowników, a nawet klientów uzyskujących dostęp do firmowych aplikacji, w połączeniu z gwałtownym wzrostem liczby naruszeń danych, podniósł poprzeczkę całemu sektorowi IT i specjalistom ds. bezpieczeństwa. W celu zapewnienia bezpiecznej wymiany informacji, organizacje IT muszą odnaleźć się w ogromnym labiryncie ludzi, procesów i technologii. Wdrażanie, konfigurowanie i utrzymywanie technologii bezpiecznego dostępu stanowi duże wyzwanie.

Systemy te są obecnie obsługiwane na zasadzie fragmentarycznej; wymagają ciągłych aktualizacji i interwencji człowieka. Nie ma jednego miejsca, z którego można by zarządzać i kontrolować technologie związane z dostępem do aplikacji. Nie ma wygodnego, prostego i szybkiego podejścia do zarządzania oprogramowaniem, sprzętem, technologiami, polityką firmy i bezpieczeństwem, które by mogło być utożsamiane z zapewnieniem bezpieczeństwa konsultantom i partnerom łańcucha dostaw. Nie ma wglądu w to, co robią osoby trzecie w Twojej sieci. Wszystkie te pojedyncze czynniki prowadzą do wzrostu ryzyka w Twojej firmie.

Konsekwencje dla przedsiębiorstwa są ogromne, a złożoność problemu i ogrom ryzyk skutkuje utratą:

- **Czasu** - zespoły ds. IT, bezpieczeństwa i zarządzania zajmują się monitorowaniem dostępu pracowników i osób trzecich do aplikacji, tracąc tym samym czas, który mogliby poświęcić na projekty o wyższym priorytecie
- **Wydajności** - pracownicy i kontrahenci stają się mniej efektywni. Na ich drodze pojawiają się komplikacje w przyznawaniu dostępu do nowych aplikacji, opóźnienia wynikające z konieczności wdrożenia nowych pracowników do objęcia nowego stanowiska. Priorytetem każdej organizacji jest posiadanie jak najbardziej efektywnych pracowników, którym realizacja tematu zajmie kilka minut, a nie dni lub tygodni.
- **Danych** - niemożność skutecznego monitorowania aktywności dostępowej w sieci może łatwo doprowadzić do naruszeń w sieci, powodujących utratę danych lub własności intelektualnej
- **Pieniędzy** - według raportu wykonawczego z 2014 r. opracowanego przez firmę HP dotyczącego naruszeń, każda utrata danych to strata średnio około 2 milionów USD.
- **Reputacji w firmie** - według ankiety Ponemon z 2014 r. dotyczącej „Następstw naruszeń danych”, naruszenia danych są w grupie 3 najważniejszych incydentów, które wpływają na reputację firmy.

UWARUNKOWANIA RYNKOWE

Dzisiejszy mobilny świat powoduje, że aby móc zachować konkurencyjność, organizacje biznesowe korzystają z zewnętrznych zasobów częściej niż kiedykolwiek przedtem. Przykładowo:

- Biuro Statystyki Pracy klasyfikuje ponad 10 milionów pracowników, w tym 7,4% siły roboczej w USA, jako niezależnych wykonawców.
- Według badań przeprowadzonych przez firmę Intuit tworzącą oprogramowanie, do 2020 r. ponad 40% amerykańskiej pracowników - lub 60 milionów ludzi - stanie się pracownikami dorywczymi.
- W 2014 r. firmy zwiększyły swoje potrzeby na zakup oprogramowania dla łańcucha dostaw o prawie 11%, wydając tym samym 9,9 miliarda dolarów.
- Wzrost liczby naruszeń w przedsiębiorstwach oraz ryzyk jakie ze sobą niosą i kosztów, to kolejna smutna prawda w dzisiejszych środowiskach biznesowych.
- Naruszenia danych w USA śledzone przez Identity Theft Resource Center (ITRC) - urząd zajmujący się analizą kradzieży tożsamości wyniosły 781 w 2015 r., drugim najwyższym rekordowym roku w historii, od momentu rozpoczęcia obserwacji w 2005 r.
- Badanie kosztów związanych z naruszeniem danych osobowych przeprowadzone przez firmę IBM w X corocznym badaniu Cost of Data Breach Study, opublikowanym w 2015 r. pokazało, że średni całkowity koszt naruszenia danych wyniósł 3,8 mln USD, co stanowi wzrost o 23% od 2013 r.
- Według raportu z 2014 roku pochodzącego z agencji kredytowej Experian, ryzyko naruszenia bezpieczeństwa danych w firmach jest wyższe niż kiedykolwiek wcześniej, a w prawie połowie badanych organizacji, w ciągu ostatnich 12 miesięcy miał miejsce przynajmniej jeden taki incydent.

DOSTĘP DO APLIKACJI W PRZEDSIĘBIORSTWIE

FIRMA AKAMAI ZMIENIA CHARAKTER ZDALNEGO DOSTĘPU I PRZYWRACA KONTROLĘ NAD NIM

Akamai podchodzi do problemu oferując organizacjom biznesowym Enterprise Application Access - usługę SaaS, która zapewnia dostęp do aplikacji bez przyznawania użytkownikom dostępu do całej sieci Twojej firmy. Z Enterprise Application Access dostęp do aplikacji jest scentralizowany i zarządzany w jednym miejscu, nie wymaga jednocześnie dodatkowego sprzętu ani oprogramowania. Zarządzanie i kontrola dostępu osób trzecich - a także klientów i pracowników - staje się prosta i uporządkowana, a co za tym idzie, zwiększa się bezpieczeństwo.

Enterprise Application Access usuwa problem w zespołach IT, które zajmują się dostępem stron trzecich do sieci. Usługa jest łatwa do wdrożenia i udostępnienia oraz zmiany i monitorowania. Enterprise Application Access eliminuje niepotrzebne elementy tj. oprogramowanie urządzenia, aktualizacje w ogóle lub aktualizacje samego oprogramowania, dodatkowy sprzęt. Znikają problemy pojawiające się w procesie administrowania kontami użytkowników - w momencie obejmowania nowego stanowiska przez pracownika i oddawania go. Jako centralny punkt kontroli Enterprise Application Access proponuje pojedynczy panel dla zarządzania finansami, widocznością, kontrolą i raportowaniem zgodności w wyniku czego otrzymujemy bezpieczny dostęp do aplikacji.

EKOSYSTEM AKAMAI

Akamai sprawia, że Internet jest szybki, niezawodny i bezpieczny. Nasze kompleksowe rozwiązania są oparte na globalnie dystrybuowanej platformie Akamai Intelligent Platform ™, zarządzanej przez ujednolicone, konfigurowalne Centrum Sterowania Luna (Luna Control Centre) w celu uzyskania widoczności i kontroli, wspieranej przez ekspertów, którzy w razie potrzeby, w miarę rozwoju strategii pomogą i zainspirują do wykorzystywania innowacyjnych rozwiązań.

advatech

Hubert Ortyl Business Development Manager Security Solutions
+ 48 607 628 862 | hortyl@advatech.pl