



Tworzenie wydajnej kosztowo sieci zgodnie z podejściem Zero Trust

Maksymalizuj bezpieczeństwo sieci i minimalizuj koszty





Cyberbezpieczeństwo i zerowe zaufanie

W miarę ciągłego postępu technologicznego oraz stale rosnącej liczby i złożoności cyberzagrożeń kwestia cyberbezpieczeństwa staje się coraz ważniejsza. Istnieją szybko zmieniające się zagrożenia, które utrudniają organizacjom przewidywanie i obronę. Wymaga to od ekspertów ds. cyberbezpieczeństwa bycia na bieżąco z najnowszymi trendami i lukami w zabezpieczeniach.

Ze względu na wiele różnych źródeł i wektorów ataków, takich jak wiadomości e-mail z próbami

phishingu, socjotechnika i luki w oprogramowaniu, ochrona przed zagrożeniami cybernetycznymi wymaga unikalnego podejścia do każdego rodzaju ataku.

Identyfikacja i ochrona wszystkich potencjalnych luk w złożonym systemie może być wyzwaniem, dlatego dla ekspertów ds. cyberbezpieczeństwa chcących opracować skuteczne środki bezpieczeństwa niezwykle ważne jest zrozumienie, w jaki sposób różne systemy i sieci współpracują ze sobą.

Błąd ludzki jest częstą przyczyną naruszeń cyberbezpieczeństwa. Szacuje się, że do 2025 r. brak kompetencji lub ludzkie niepowodzenie będą odpowiedzialne za ponad połowę znaczących incydentów cybernetycznych.¹

Spełnienie złożonych przepisów i standardów cyberbezpieczeństwa, takich jak ogólne rozporządzenie o ochronie danych (RODO) oraz ustawa o przenośności i odpowiedzialności w ubezpieczeniach zdrowotnych (HIPAA), to kolejne wyzwanie wymagające specjalistycznej wiedzy i doświadczenia.

1 Gartner® Predicts 2023: Cybersecurity Industry Focuses on the Human Deal | Bitsight, styczeń 2023 r.

Krótki opis rozwiązania

Tworzenie wydajnej kosztowo sieci zgodnie z podejściem Zero Trust



Proces naruszenia cyberbezpieczeństwa

Poniższy schemat przedstawia etapy działania cyberprzestępcy, który chce włamać się do sieci i ukraść cenne dane. Zaczyna się od rozpoznania, podczas którego napastnicy badają, identyfikują i wybierają cele oraz skanują je pod kątem luk w zabezpieczeniach sieci.

Następnym etapem jest uzbrojenie, podczas którego atakujący ustalają, w jaki sposób naruszyć zabezpieczenia docelowego punktu końcowego i dostarczyć uzbrojony ładunek.

Potem następuje wykorzystanie, podczas którego atakujący uruchamia uzbrojony ładunek i zwiększa uprawnienia w zaatakowanym punkcie końcowym, aby móc poruszać się po sieci.

Kolejny etap to instalacja, podczas której atakujący uzyskują zdalny dostęp do powłoki i instalują złośliwe oprogramowanie w celu uzyskania trwałości.

Na etapie dowodzenia i kontroli napastnicy ustanawiają zaszyfrowane kanały komunikacyjne z powrotem do serwerów dowodzenia i kontroli, aby zdalnie kierować atakiem i realizować cele.

Ostatnim etapem jest ruch boczny i eksfiltracja, podczas którego atakujący mogą mieć wiele celów, w tym kradzież danych, zniszczenie lub modyfikację krytycznych systemów i odmowę usługi.

Kluczem do powstrzymania atakujących jest wczesne wykrycie różnych etapów cyklu życia ataku i zakłócenie ich przebiegu.

Aby temu zapobiec, należy podjąć szereg działań, takich jak zarządzanie lukami w zabezpieczeniach i poprawkami, wykrywanie złośliwego oprogramowania i udaremnianie jego działań, blokowanie ryzykownych aplikacji i usług oraz rejestrowanie i monitorowanie całej sieci, punktów końcowych i oczywiście aktywności w chmurze.

Po stronie sieci konieczne jest wdrożenie technologii zapewniających szczegółową kontrolę aplikacji i monitorowanie ruchu pomiędzy strefami lub segmentami w ramach modelu zerowego zaufania. Zerowe zaufanie działa na zasadzie, że wszystko należy domyślnie uważać za niegodne zaufania.

Koncepcja zerowego zaufania została opracowana w odpowiedzi na rosnącą liczbę wyrafinowanych cyberataków na sieci komputerowe. Tradycyjnie w celu ochrony swoich sieci organizacje polegały na rozwiązaniach bezpieczeństwa działających na granicach sieci, takich jak zapory ogniowe i oprogramowanie antywirusowe. Jednakże w miarę jak cyberataki stawały się bardziej zaawansowane i złożone, rozwiązania stosowane na granicy sieci okazały się niewystarczające. Obecnie każde żądanie dostępu musi zostać zweryfikowane i uwierzytelnione przed udzieleniem dostępu do zasobów.



Źródło: [XDR for Dummies, Palo Alto Networks Special Edition, 2022](#)

Krótki opis rozwiązania

Tworzenie wydajnej kosztowo sieci zgodnie z podejściem Zero Trust



Udoskonalanie strategii zerowego zaufania

Alcatel-Lucent Enterprise pomaga klientom zwiększyć bezpieczeństwo i przejść do środowiska zerowego zaufania dzięki prostocie i oszczędności. W ALE rozumiemy, jak ważne jest wdrożenie modelu zerowego zaufania w celu zapewnienia bezpieczeństwa sieci i danych naszych klientów. Oferujemy szereg rozwiązań mających pomóc organizacjom wdrożyć sieć o zerowym zaufaniu i stawić czoła wyzwaniom, jakimi są zagrożenia cybernetyczne.

Wzmacnianie sieci

Oferujemy **sieć wzmocnioną – zarówno wewnątrz, jak i na zewnątrz**. Wzmacnianie zaczyna się od bezpiecznej infrastruktury i upewnienia się, że samo urządzenie nie jest zagrożone. Nasza rodzina produktów [Alcatel-Lucent OmniSwitch®](#) działa w oparciu o bezpieczny system operacyjny Alcatel-Lucent (AOS), który wykorzystuje bezpieczny, zróżnicowany kod do ochrony sieci przed potencjalnymi lukami w zabezpieczeniach i atakami. Kod jest stale aktualizowany w celu uwzględnienia obecnych i przyszłych zagrożeń, przy dywersyfikacji oprogramowania poprzez randomizację układu przestrzeni adresowej (ASLR) wykorzystywaną do ochrony przed atakami związanymi z przepełnieniem bufora. Niezależna weryfikacja i walidacja (IV&V) służy również do analizy i testowania kodu źródłowego AOS pod kątem potencjalnych luk w zabezpieczeniach, backdoorów, złośliwego oprogramowania i exploitów systemowych. Zewnętrzni eksperci ds. cyberbezpieczeństwa przeprowadzają te testy, wykonywane na ogólnie dostępnych obrazach oprogramowania, aby zapewnić jego integralność.

Stosujemy makro- i mikrosegmentację, aby zapewnić dostęp do sieci o zerowym zaufaniu. Obydwie strategie są kluczowymi elementami strategii bezpieczeństwa zerowego zaufania.

Makrosegmentacja oznacza podział sieci na oddzielne strefy lub domeny w oparciu o funkcję, aplikację lub grupę użytkowników. Zapewnia to wysoki poziom segmentacji sieci, umożliwiając organizacjom odizolowanie krytycznych zasobów i zasobów od reszty sieci. Z drugiej strony **mikrosegmentacja** koncentruje się na segmentacji sieci na bardziej szczegółowym poziomie, aż do pojedynczego użytkownika lub urządzenia. Takie podejście zapewnia bardziej precyzyjną kontrolę nad dostępem do sieci, umożliwiając organizacjom egzekwowanie zasad bezpieczeństwa na poziomie pojedynczego użytkownika lub urządzenia.

[Protokół Shortest Path Bridging \(SPB\)](#) i **uniwersalne profile sieciowe (UNP)** stanowią zaawansowane rozwiązanie wspierające makro- i mikrosegmentację sieci, co poprawia bezpieczeństwo i wydajność poprzez ograniczenie zakresu potencjalnych ataków.

SPB to protokół sieciowy w warstwie 2., który umożliwia routing wielościżkowy w dużych sieciach, upraszczając jednocześnie konfigurację i zarządzanie infrastrukturą sieciową. Funkcje takie jak segmentacja sieci wirtualnej zapewniają dodatkową ochronę przed nieautoryzowanym dostępem i cyberatakami. Wykorzystując SPB w swojej infrastrukturze sieciowej, organizacje mogą czerpać korzyści z zwiększonej wydajności i bezpieczeństwa sieci, co sprzyja pewnemu osiągnięciu celów biznesowych.

ALE UNP to kontrola dostępu oparta na profilach, zaawansowana funkcja przełącznika Alcatel-Lucent Enterprise, która umożliwia administratorom sieci tworzenie profili użytkowników i zarządzanie nimi w celu uzyskania dostępu do sieci w oparciu o tożsamość, lokalizację i urządzenie. Mogą oni wdrażać scentralizowane zarządzanie zasadami sieciowymi, upraszczając konfigurację i egzekwowanie zasad. Wdrażając ALE UNP, organizacje mogą zwiększyć widoczność, bezpieczeństwo i kontrolę swojej sieci, jednocześnie poprawiając jej wydajność, chroniąc zasoby i skracając przestoje.

Razem SPB i UNP umożliwiają administratorom sieci efektywne zarządzanie infrastrukturą sieciową i zabezpieczanie jej w celu spełnienia następujących postulatów:

- Konsekwentnie stosuj zasady w całej sieci
- Segmentuj i izoluj urządzenia IoT od innych urządzeń
- Zminimalizuj powierzchnię potencjalnego ataku w sieci

Krótki opis rozwiązania

Tworzenie wydajnej kosztowo sieci zgodnie z podejściem Zero Trust



Solidne uwierzytelnianie

ALE zapewnia niezawodne uwierzytelnianie za pośrednictwem systemu zarządzania uwierzytelnianiem w oparciu o ujednoliconą politykę (Unified Policy Authentication Manager, UPAM).

Kluczowym elementem cyberbezpieczeństwa jest uwierzytelnianie, czyli proces weryfikacji tożsamości użytkownika, urządzenia lub systemu. Polega ono na potwierdzeniu, że użytkownik lub urządzenie jest tym, za kogo się podaje, zwykle poprzez podanie jakiejś formy identyfikacji, takiej jak nazwa użytkownika i hasło.

Rozwiązanie ALE obsługuje wiele metod uwierzytelniania użytkowników.

- 802.1X, protokół uwierzytelniania sieciowego, umożliwia urządzeniom łączenie się z bezpieczną siecią poprzez podanie poświadczeń, takich jak nazwa użytkownika i hasło. Gdy urządzenie próbuje połączyć się z siecią przy użyciu protokołu 802.1X, zostaje uwierzytelnione, zanim uzyska dostęp do sieci. W idealnym świecie urządzenie uwierzytelnia się za pomocą protokołu 802.1X.

Uwierzytelnianie generuje rekord, który można udostępnić zaporze.

- Jeśli urządzenie nie obsługuje protokołu 802.1X, dostępna jest opcja uwierzytelniania za pomocą adresu MAC. Adres MAC to cyfrowy identyfikator każdego urządzenia w sieci. Jest on niepowtarzalny i identyfikuje każde urządzenie oraz umożliwia komunikację między nimi, podobnie jak plakietka na komputer lub telefon.
- ALE obsługuje cyfrowy fingerprinting urządzeń i systemów. Jeśli przy innym uwierzytelnieniu 802.1X lub MAC nie zostanie zwrócony żaden profil, podejmiemy próbę cyfrowego fingerprintingu. Cyfrowy fingerprinting w systemie bezpieczeństwa komputera to proces gromadzenia informacji o urządzeniu lub systemie, takich jak jego system operacyjny, oprogramowanie i otwarte porty, w celu jego identyfikacji i kategoryzacji oraz oceny potencjalnych zagrożeń i luk w zabezpieczeniach. Proces ten można także wykorzystać do mapowania na profil urządzenia zarejestrowanego w bazie danych inwentaryzacji urządzeń IoT.

- ALE zapewnia także opcję domyślną „catch all” w przypadku, gdy nie uda się znaleźć żadnego profilu. Domyślna reguła catch-all może zezwalać na ograniczony dostęp lub całkowicie odmówić dostępu, jeśli podstawowe uwierzytelnianie zakończy się niepowodzeniem.

Aby realizować te różne typy uwierzytelniania, potrzebujesz miejsca do tworzenia poświadczeń użytkowników i urządzeń oraz zarządzania nimi. Potrzebny jest do tego UPAM, składnik rozwiązania Ujednolicony Dostęp ALE. Zapewnia on scentralizowane usługi uwierzytelniania, autoryzacji i rozliczania (AAA) dla sieci. Umożliwia administratorom sieci tworzenie profili użytkowników w celu uzyskiwania dostępu do sieci i zarządzanie nimi, między innymi w oparciu o tożsamość i lokalizację. Usługę UPAM można konfigurować i zarządzać nią za pomocą [systemu zarządzania siecią Alcatel-Lucent OmniVista®](#), dzięki czemu administratorzy sieci mogą definiować i egzekwować zasady dostępu do sieci.

Krótki opis rozwiązania

Tworzenie wydajnej kosztowo sieci zgodnie z podejściem Zero Trust



Reagowanie na incydenty

Szybkie reagowanie na incydenty sieciowe jest kluczowym czynnikiem minimalizującym uszkodzenia systemów i sieci, a także skracającym przestoje spowodowane atakami, takimi jak rozproszona odmowa usługi (Distributed Denial of Service, DDoS).

Minimalizuj ryzyko, maksymalizuj jakość obsługi (QoE) i zwiększaj bezpieczeństwo dzięki [doradcy sieciowemu Alcatel-Lucent OmniVista Network Advisor](#). OmniVista Network Advisor to inteligentny i autonomiczny system oparty na sztucznej inteligencji, który umożliwia monitorowanie sieci w czasie rzeczywistym, wysyłanie alertów w razie problemów i sugerowanie rozwiązań różnych problemów związanych z siecią i bezpieczeństwem, w tym ataków DDoS. System stale przeprowadza audyty konfiguracji i analizy wydajności sieci, dzięki czemu może szybko identyfikować potencjalne problemy, zwalczać je i optymalizować sieć przy minimalnym zaangażowaniu działu IT lub wręcz bez jego udziału.

Partnerstwa i integracje

Ważnym aspektem uwierzytelniania jest integracja z zaporami sieciowymi. Na przykład dzięki integracji z Fortinet użytkownicy lub urządzenia

uwierzytelnieni w sieciach LAN i/ lub WLAN mogą być jednocześnie i bezproblemowo uwierzytelniani w zaporze Fortinet.

Dzięki integracji zapory nowej generacji firmy Palo Alto Networks (PAN) użytkownicy lub urządzenia uwierzytelniane w sieciach LAN i/ lub WLAN mogą być jednocześnie i bezproblemowo uwierzytelniane w zaporze PAN.

Nasza współpraca z firmą [Versa Networks](#) umożliwia bezpieczny dostęp do kluczowych zasobów niezależnie od lokalizacji użytkowników, danych, aplikacji i urządzeń. Jest to szczególnie korzystne dla firm, których biura regionalne lub oddziały są oddalone od lokalizacji centralnej lub centrum danych. W przeciwieństwie do tradycyjnych rozległych sieci komputerowych (WAN), które wymagają wielu przeskoków w sieci i mogą wiązać się z dodatkowymi kosztami, SASE i SD-WAN stanowią ekonomiczne i bezpieczne rozwiązanie w erze transmisji client-to-cloud. Łącząc te dwa rozwiązania, firmy mogą uprościć zarządzanie infrastrukturą IT i umożliwić bezpieczny dostęp do internetu i aplikacji biznesowych w scenariuszach pracy z dowolnego miejsca, w tym w przedsiębiorstwie/ DC, biurach regionalnych/oddziałach

oraz pracownikom domowym/ mobilnym.

[Oferta ALE-Versa Titan](#) to kompleksowe rozwiązanie, które łączy usługi krawędzi usługi bezpiecznego dostępu (Secure Access Service Edge, SASE) i SD-WAN z chmury. Obejmuje ono Versa Titan SD-WAN, który zapewnia oparty na chmurze SD-WAN dla oszczędnego IT, a także usługę Versa Secure Access (VSA), oferującą funkcje zapory ogniowej nowej generacji i blokowanie geograficzne, a także dostęp do sieci o zerowym zaufaniu (Zero Trust Network Access, ZTNA) do scenariuszy pracy z dowolnego miejsca. Ponadto Versa Secure Web Gateway (SWG) zapewnia bezpieczne przeglądanie stron internetowych i dostęp do aplikacji internetowych (SaaS) w celu zapewnienia bezpiecznej łączności zdalnej z biurem domowym. Portal internetowy i aplikacja Versa Titan oferują zintegrowane usługi sieciowe i bezpieczeństwa na jednej platformie, a wszystkie komponenty SASE pochodzą od tego samego dostawcy. Dzięki jednemu repozytorium zasad obejmującemu zasady dotyczące sieci i bezpieczeństwa firmy mogą uprościć zarządzanie zasobami informatycznymi i zapewnić bezpieczny dostęp do krytycznych zasobów.

Krótki opis rozwiązania

Tworzenie wydajnej kosztowo sieci zgodnie z podejściem Zero Trust



Metodologia zerowego zaufania

Aby wdrożyć model zerowego zaufania, organizacje muszą najpierw zająć się problemami w istniejącej infrastrukturze bezpieczeństwa, takimi jak niespójne zasady, domyślne zaufanie i podatne na ataki urządzenia IoT. Celem jest ustanowienie dostępu do sieci oraz możliwości kontroli dostępu opartej na rolach, segmentacji i monitorowania w celu rozwiązania tych problemów, przy odpowiedniej segmentacji umożliwiającej podział wrażliwych zasobów i ograniczenie dostępu tylko do tych, którzy go potrzebują. Funkcje monitorowania i kwarantanny umożliwiają klientom identyfikację i izolowanie potencjalnych zagrożeń.

Prosta, ale wydajna metodologia budowania sieci o zerowym zaufaniu za pomocą rozwiązań ALE obejmuje kilka etapów.

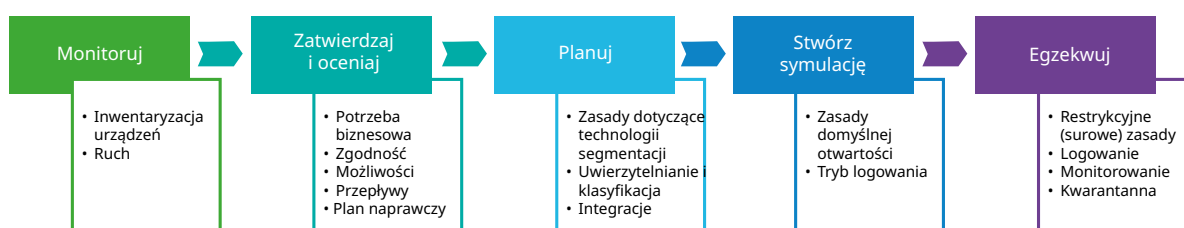
- **Monitoruj:** należy prowadzić monitorowanie, w tym stanu urządzeń i ruchu
- **Zatwierdź i oceniaj:** zatwierdzanie i ocena obejmują analizę potrzeb biznesowych, wymagań dotyczących zgodności, możliwości i przepływów
- **Planuj:** na podstawie wyników oceny należy stworzyć plan naprawczy. Planowanie obejmuje wybór właściwej technologii i zasad segmentacji, a także rozważenie uwierzytelniania w kontekście klasyfikacji oraz integracji.
- **Stwórz symulację:** na etapie symulacji zasady są domyślnie otwarte i działają w trybie logowania, a inne funkcje są testowane
- **Egzekwuj:** etap egzekwowania obejmuje wdrażanie restrykcyjnych zasad, rejestrowanie, monitorowanie i przeprowadzanie działań związanych z kwarantanną

Całkowity koszt posiadania (TCO)

Całkowity koszt posiadania (TCO) obejmuje wszystkie wydatki związane z posiadaniem i obsługą produktu lub usługi przez cały okres ich użytkowania. Należą do nich między innymi cena zakupu, konserwacja, wsparcie i aktualizacje. Ważne jest, aby wybierać opłacalne rozwiązania oferujące długoterminową wartość, co może zapobiec przekroczeniu budżetu i zapewnić lepszy zwrot z inwestycji (ROI).

Należy uwzględnić rozróżnienie pomiędzy początkową inwestycją kapitałową a bieżącymi wydatkami koniecznymi do utrzymania licencji i funkcjonalności systemu. Niektóre komponenty, takie jak zapory ogniowe, skupiają się wyłącznie na bezpieczeństwie, natomiast inne są również kluczowe dla zbudowania bardziej szczegółowej strategii bezpieczeństwa. Należą do nich zarządzanie strategiami, wydajna technologia separacji ścieżek sieci (zaawansowana i zautomatyzowana makro- i mikrosegmentacja), automatyczne przypisywanie sieci wirtualnej (VLAN), protokół szyfrowania sieci, widoczność aplikacji oraz niezależna walidacja i atestacja kodu systemu operacyjnego.

Strategia ALE w zakresie cyberbezpieczeństwa sieci obejmuje wspomniane powyżej istotne elementy bezpieczeństwa sieci bez żadnych kosztów, podczas gdy alternatywy innych dostawców wymagają specjalistycznej wiedzy oraz wielu kosztownych elementów i licencji na eksploatację i utrzymanie. Podejście ALE zapewnia klientom znaczne korzyści ekonomiczne, a zarazem solidne i wydajne cyberbezpieczeństwo sieci.



Krótki opis rozwiązania

Tworzenie wydajnej kosztowo sieci zgodnie z podejściem Zero Trust



Wniosek

Jest oczywiste, że wdrożenie sieci o zerowym zaufaniu w celu zapewnienia solidnego poziomu bezpieczeństwa może wiązać się z kilkoma wyzwaniami, takimi jak złożoność i koszty w zakresie tworzenia i utrzymania sieci. Jednak ALE oferuje unikalne i opłacalne podejście do rozwiązania tych problemów. Oprócz innych komponentów przedstawionych w tym dokumencie, zaawansowane technologie makro- i mikrosegmentacji zapewniają prosty i niedrogi sposób na wdrożenie sieci o zerowym zaufaniu, która spełnia współczesne wymagania cyberbezpieczeństwa. Chcemy wspierać naszych klientów w rozwiązywaniu ich problemów związanych z cyberbezpieczeństwem i wierzymy, że nasze podejście może pomóc w osiągnięciu tego celu.

Rozwiązania ALE obejmują naszą odporną i bezpieczną [technologię Intelligent Fabric \(iFab\)](#) i UNP oraz solidną kontrolę dostępu do sieci (NAC) z UPAM, zapewniającą kontrolę dostępu opartą na profilach. Nasze innowacyjne rozwiązanie [OmniVista Network Advisor](#) zapewnia płynność działania oraz szybkie przywracanie funkcji i zapobieganie atakom. Ponadto współpracujemy z dostawcami SASE, takimi jak Versa Networks, i integrujemy się z dostawcami zapór sieciowych, takimi jak Palo Alto Networks, aby zapewnić klientom bardziej kompleksowe i zintegrowane rozwiązania z zakresu bezpieczeństwa.

