



Architektura Zero Trust



Spis treści

Czym jest architektura Zero Trust?.....	3
Zrozumienie makro- i mikrosegmentacji	5
Dlaczego obydwa rodzaje segmentacji są potrzebne	6
Jak wprowadzić model bezpieczeństwa Zero Trust	7
Metodologia.....	7
Jeszcze jedna rzecz	12
Dlaczego ALE?.....	12
Co wiemy na pewno.....	13



Czym jest architektura Zero Trust?

Co oznacza architektura Zero Trust (ZTA)? Oznacza to, że każdy użytkownik i urządzenie musi zostać uwierzytelniony i autoryzowany przed zezwoleniem na dostęp do danych. To strategia: „Nie ufaj nikomu, uwierzytelniaj wszystko”.

Pomocna może być pewna analogia.

Jeśli tradycyjne bezpieczeństwo jest fortecą, która chroni wioskę, wokół wioski (inaczej zwanej przedsiębiorstwem) zbudowalibyśmy mur forteczny (inaczej zwany zaporą). Wszystko, co pochodzi z zewnątrz nie budzi zaufania i jest poddawane kontroli, natomiast wszystko, co wewnątrz, jest z założenia godne zaufania i dozwolone. Ta granica zaufania jest zarówno fizyczna, jak i dorozumiana, w zależności od tego, po której stronie twierdzy się znajdujesz, ponieważ dopóki znajdujesz się po „właściwej” stronie muru, żadne kolejne kontrole nie są konieczne. Stosując to podejście w kontekście sieci korporacyjnej, widzimy, że może istnieć pewna podstawowa segmentacja w postaci sieci VLAN, identyfikatorów SSID, podsieci lub interfejsów powiązanych z zaporą ogniową, ale ta segmentacja jest statyczna i ma więcej wspólnego ze skalowalnością sieci i możliwością zarządzania niż z bezpieczeństwem.

Obecnie jednak stosowanie zapory ogniowej (fortecy) z wielu powodów staje się samo w sobie mniej skuteczne. Pierwszy to mobilność. Użytkownicy łączą się z innymi sieciami poza firmą, co może nieść ze sobą zagrożenia. Po drugie, goście niekoniecznie są godni zaufania. Można by twierdzić, że nawet pracownikom (tym wewnątrz twierdzy) nie należy ślepo ufać. Po trzecie, do sieci dodawanych jest coraz więcej urządzeń IoT. Stanowią one większe zagrożenie dla bezpieczeństwa, ponieważ mogą nie podlegać sankcjom i zarządzaniu przez dział IT, a także zazwyczaj nie posiadają funkcji bezpieczeństwa. W przypadku tradycyjnego podejścia „twierdza/wioska”, czyli „zapora/przedsiębiorstwo”, jeśli użytkownik lub urządzenie stanie się celem ataku, niewiele lub nic nie powstrzyma zagrożenia przed rozprzestrzenieniem się na innych użytkowników i urządzenia. Gdy dostaniesz się do środka, możesz się swobodnie poruszać.

Wracając do analogii z fortecą: jeśli jedyną rzeczą chroniącą wioskę przed intruzami jest mur, to w dniu, w którym intruzi nauczą się wspinać na mur fortecy — co na pewno nastąpi — dojdzie do katastrofy.





Pytanie brzmi – co możemy z tym zrobić? Pomyślmy o tym z perspektywy, którą można określić jako „nie ufaj nikomu” lub „zero zaufania”.

W przypadku zerowego zaufania żaden użytkownik ani urządzenie nie są godne zaufania. Niezależnie od tego, czy znajdują się w lokalizacji firmy, czy poza nią, przechodzą te same kontrole. Nie ma czegoś takiego, jak godni zaufania użytkownicy wewnętrzni. Każdy dostęp wymaga uwierzytelnienia i upoważnienia.

W analogii z fortecą oznaczałoby to, że oprócz fortecy, która chroni wioskę przed zagrożeniami z zewnątrz, każdy dom, każdy budynek ma swoje własne zabezpieczenie przed zagrożeniami ze strony nikiemnych aktorów mieszkających w twierdzy. Jeśli chodzi o Enterprise, tak zwana mikrosegmentacja definiowana programowo idzie o krok dalej. Oprócz fortecy i ochrony budynków mamy również osobistych ochroniarzy, którzy podążają wszędzie za nami. A gdziekolwiek się udamy, musimy okazać paszport. W sieci Enterprise ta granica zaufania jest rozmyta, rozproszona i mobilna. Nie jest powiązana z konkretną lokalizacją, portem przełącznika ani siecią VLAN. Zależy między innymi od tożsamości, urządzenia, sytuacji i pory dnia. Jest definiowana przez oprogramowanie i na bieżąco modyfikowana. Zgodnie z tym podejściem komponenty muszą być zarządzane i powinny być w stanie zmieniać konfigurację w razie potrzeby, aby reagować na zagrożenia lub zmiany w przepływie pracy.



Zrozumienie makro- i mikrosegmentacji

W architekturze zerowego zaufania istnieją dwa rodzaje segmentacji: makro- i mikrosegmentacja. Według naszej analogii mur fortecy to makrosegmentacja, a osobiści ochroniarze to mikrosegmentacja.

Makrosegmentacja **polega** na podziale sieci fizycznej na różne segmenty logiczne. Te segmenty mogą korzystać z VLAN, kombinacji VLAN i VRF, a także VPN, gdy mówimy o protokole SPB, MPLS, a nawet tunelach VXLAN lub GRE. Zapora kontroluje wszelki ruch między użytkownikami lub urządzeniami w różnych segmentach. Wszystkie przedsiębiorstwa stosują segmentację w takiej czy innej postaci, ale nie zawsze ze względów bezpieczeństwa. Dość często ten rodzaj segmentacji jest stosowany ze względu na skalowalność, kwestie administracyjne lub organizacyjne. Jeśli dwa urządzenia są mapowane do różnych sieci VLAN, ale mogą komunikować się bez przechodzenia przez zaporę, znajdują się one w tym samym segmencie makro. Typowym przykładem tego rodzaju segmentacji jest prowadzenie telefonii IP w oddzielnych sieciach VLAN i VRF, które są logicznie odizolowane od komputerów PC.

Pytanie brzmi: jak zmapować użytkowników lub urządzenia do tych segmentów? Chociaż można to zrobić statycznie, np. za pomocą portu przełącznika lub identyfikatora SSID, ten sposób naprawdę przestarzały. Jest za mało elastyczny i nie wróży dobrze użytkownikom mobilnym. Idealnie byłoby, gdyby istniał system uwierzytelniania definiowany programowo, w którym do użytkownika lub urządzenia w momencie łączenia się i uwierzytelniania byłby przypisywany profil. Profil udostępni użytkownika lub urządzenie we właściwym segmencie, niezależnie od fizycznej lokalizacji, portu przełącznika lub identyfikatora SSID.

Chociaż makrosegmentacja przynosi korzyści w zakresie bezpieczeństwa, w wielu przypadkach jest stosowana ze względów organizacyjnych lub administracyjnych. Na przykład kamery i zamki do

drzwi mogą podlegać kontroli grupy bezpieczeństwa dostępu, podczas gdy termostaty mogą podlegać kontroli grupy konserwacji budynku.

Mikrosegmentacja idzie o krok dalej. Nie wszyscy użytkownicy są tacy sami i nie wszyscy użytkownicy mają uzasadnioną potrzebę dostępu do wszystkich zasobów. Ten sam profil, który mapuje użytkowników do segmentu, obejmuje również zestaw zasad zapewniających drobiazgową kontrolę nad uprawnieniami użytkowników/urządzeń, które różnią się w zależności od roli, np. HR lub Finanse. Rozwiązanie to znane jest jako „**dostęp oparty o rolę**” i jest bezpośrednio związane z „**zasadą najmniejszego uprzywilejowania**”. Zatem mimo, że kamery i zamki do drzwi znajdują się w tym samym segmencie, nie muszą korzystać z tych samych zasobów. Kamera musi komunikować się z rejestratorem obrazu, a zamek w drzwiach – z serwerem. Nie ma potrzeby, aby kamera komunikowała się z zamkiem drzwi, tak jak nie ma potrzeby, aby zamek drzwi komunikował się z innym zamkiem drzwi. Te szczegółowe uprawnienia są wdrażane przy użyciu zasad, które są częścią profilu i zostają dynamicznie zastosowane do urządzenia po uwierzytelnieniu.

Mikrosegmentacja musi być zdefiniowana programowo z kilku powodów. Ani użytkownicy, ani urządzenia IoT nie są statyczne, poruszają się, łączą i rozłączają, stosowane strategie nie mogą być powiązane z lokalizacją lub portem. W rzeczywistości konfiguracje mikrosegmentacji muszą być dynamiczne w oparciu o kombinację wielu czynników, w tym między innymi tożsamości użytkownika lub urządzenia, pory dnia i lokalizacji.

Podsumowując: gdy komunikacja pomiędzy różnymi segmentami jest kontrolowana przez zaporę, jest to makrosegmentacja. Gdy komunikacja w ramach tego samego segmentu jest kontrolowana przez strategię kontroli dostępu do sieci (NAC) powiązane z urządzeniem lub rolą użytkownika, jest to mikrosegmentacja.



Dlaczego obydwa rodzaje segmentacji są potrzebne

Co się stanie, jeśli użyjesz tylko jednego rodzaju segmentacji?

Przyjrzyjmy się makrosegmentacji. Problem ze stosowaniem wyłącznie tego podejścia polega na tym, że zaporę staje się wąskim gardłem, ponieważ cały ruch musi przechodzić przez zaporę w celu uwierzytelnienia i autoryzacji. Może to powodować problemy z wydajnością. W warstwie dystrybucyjnej można wdrożyć więcej zapór, ale może to być dość kosztowne i niekoniecznie poprawiać wydajność, ponieważ zapory nie mają szybkości połączeń. Ponadto istnieje wówczas wiele punktów egzekwowania zasad i wiele miejsc, w których można aktualizować zasady, co utrudnia zarządzanie.

Druga opcja, wykorzystująca jedynie mikrosegmentację, również jest problematyczna. Jeśli egzekwowanie zasad odbywa się jedynie przy użyciu kontroli dostępu do sieci (NAC), listy zasad stają się bardzo długie i złożone oraz mogą wyczerpać limity pojemności urządzenia.

Najważniejsze jest to, że lepiej utrzymywać równowagę między tymi dwiema formami segmentacji. Niech zaporę kontroluje wszelki ruch między różnymi segmentami (pionowy), a zasady NAC – ruch w danym segmencie (poziomy).

Łącząc obydwa rodzaje segmentacji, można przeciwdziałać zagrożeniom bezpieczeństwa, które przenoszą się z jednego segmentu bezpieczeństwa do drugiego, a także takim, które przemieszczają się poziomo w tym samym segmencie. Mówiąc bardziej obrazowo, mikrosegmentacja uniemożliwia napastnikowi, któremu udało się włamać, wykorzystanie naruszenie jako trampoliny do naruszenia innych zasobów, takich jak zamek w drzwiach.

Celem jest uwierzytelnianie każdego połączenia i przypisywanie uprawnień każdemu użytkownikowi lub urządzeniu. Oznacza to stosowanie segmentacji w celu zapobiegania rozprzestrzenianiu się zagrożeń poprzez ruch poprzeczny oraz ciągłe monitorowanie i kwarantannę każdego użytkownika lub urządzenia, które przestaje spełniać wymagania.





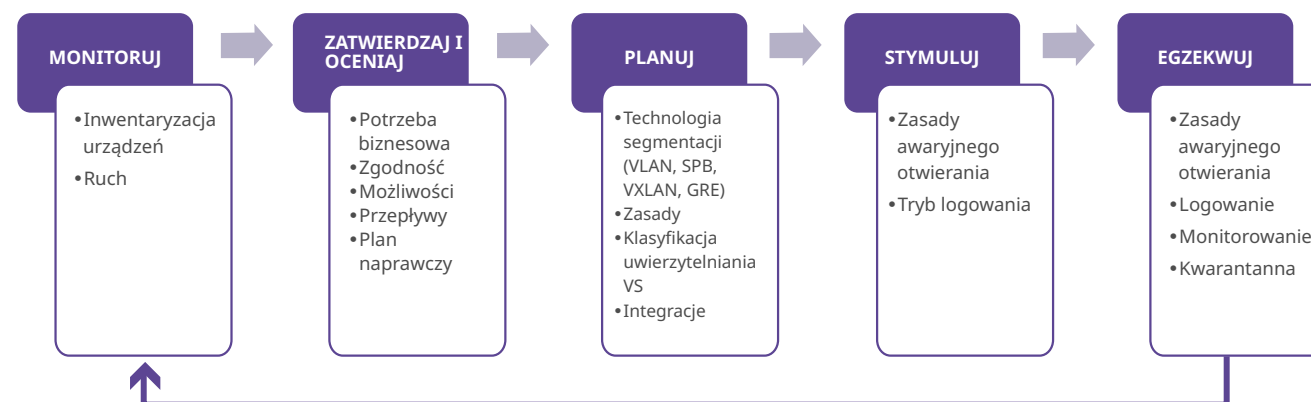
Jak wprowadzić model bezpieczeństwa Zero Trust

Działając od podstaw, stosunkowo łatwo byłoby zbudować architekturę Zero Trust, stosując mikrosegmentację od samego początku. Jednak w sytuacjach zastanych wyposażenie sieci w mikrosegmentację może spowodować zablokowanie użytkowników, urządzeń i aplikacji z powodu nieudanych uwierzytelnień lub niekompletnych strategii. Przeprowadzenie przez firmę migracji za jednym zamachem — w jednym cyklu odświeżania — byłoby trudne lub wręcz mało prawdopodobne.

W środowiskach zastanych nastąpi okres, w którym architektury niezerowego i zerowego zaufania będą współistnieć, a migracja będzie odbywać się w jednej warstwie lub w jednej lokalizacji na raz. Ważne jest, aby wdrażanie elementów infrastruktury oraz sposób ich wdrażania był elastyczny i umożliwiał działanie w trybie zerowego zaufania lub w trybie mikrosegmentów, gdy inne elementy infrastruktury są gotowe. Oznacza to, że infrastruktura będzie musiała współpracować z istniejącymi i przyszłymi komponentami.

Metodologia

Istnieje pięć kroków w kierunku architektury Zero Trust – monitorowanie, weryfikacja i ocena, planowanie, symulacja i egzekwowanie.



Rysunek 1 – Metodologia



Krok 1: Monitorowanie

Zanim przystąpisz do innych działań, musisz zacząć monitorować oraz tworzyć mapę i spis tego, co masz w swojej sieci.

Migracja do architektury ZTA wymaga szczegółowej znajomości zasobów (fizycznych i wirtualnych), podmiotów (w tym uprawnień użytkowników) oraz procesów biznesowych dotyczących sieci i odbywających się w niej. Niepełna wiedza najczęściej jest przyczyną niepowodzeń, gdy dochodzi do odmowy dostępu z powodu niewystarczających informacji. Stanowi to problem zwłaszcza wtedy, gdy w organizacji funkcjonują nieoficjalne elementy IT lub IoT.

Zacznij monitorować urządzenia i przepływy ruchu. Utwórz raport z inwentaryzacji ze wszystkimi urządzeniami widocznymi w sieci, z podziałem na m.in. typy urządzeń, producentów, modele i systemy operacyjne. Raport powinien również wskazywać, gdzie i na którym porcie przełącznika lub identyfikatorze SSID urządzenie było ostatnio widziane. Informacje te można gromadzić na podstawie takich elementów, jak adres MAC, podpis DHCP i agent użytkownika HTTP.

Większość narzędzi innych firm poda tylko adres IP, a nie typ sprzętu. Idealnie byłoby mieć narzędzie do tworzenia inwentaryzacji IoT/urządzeń, ułatwiające szybkie i łatwe tworzenie profili NAC dla każdego typu urządzenia.

Inną informacją potrzebną do tworzenia strategii są przepływy ruchu. W zależności od posiadanego sprzętu możesz uzyskać te informacje przy użyciu narzędzi do monitorowania przepływu, takich jak sFlow, Netflow lub Deep Packet Inspection (DPI).

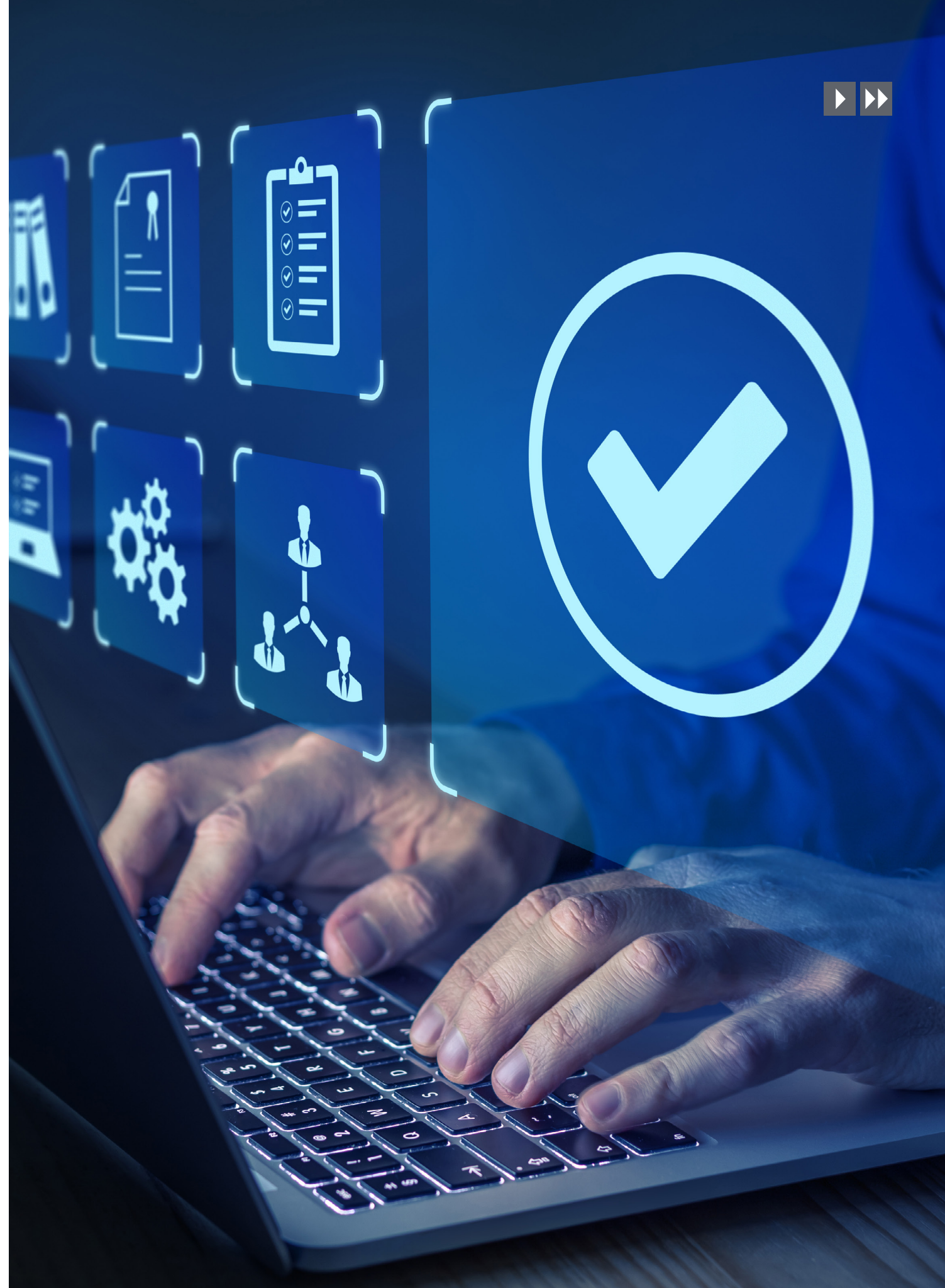
Proces ten ma charakter iteracyjny. Gdy po raz pierwszy włączysz monitorowanie, raporty jeszcze nieść ze sobą niewiele treści, ale w miarę przechodzenia do kolejnych kroków staną się one bardziej szczegółowe i przydatne. Informacje zebrane na tym etapie będą kluczowe dla kolejnych czynności.



Krok 2: Zatwierdzanie i ocena

Następny krok polega na weryfikacji tych ustaleń. Oceniaj potrzeby biznesowe. Wszelkie nieoficjalne urządzenia IoT, których obecności nie można uzasadnić, należy wyeliminować, ponieważ niepotrzebnie zwiększają powierzchnię ataku. Co do reszty, musisz zdefiniować podmioty (użytkowników i urządzenia), przepływy ruchu i przepływy pracy, ponieważ będą one musiały zostać ujęte w Twoich zasadach. Na przykład: kto będzie miał dostęp do określonych zasobów i co będzie mógł z nimi zrobić. Zastosuj zasadę jak najmniejszych przywilejów.

Mikrosegmentacja nie oznacza poluzowania innych zasad bezpieczeństwa, takich jak zasady dotyczące haseł lub aktualizacje oprogramowania firmowego. Należy ocenić możliwości poszczególnych urządzeń. Czy urządzenia te obsługują uwierzytelnianie oparte na certyfikatach? Czy istnieje narzędzie do zarządzania, które pozwoli na wydawanie i stosowanie tych certyfikatów? Jakie są wymagane przepływy ruchu? Być może trzeba będzie uzyskać te informacje od producenta, ale należy również porównać je z własnymi raportami analizy ruchu. Jeśli znajdziesz zasoby niezgodne z zasadami firmy, potrzebujesz planu naprawczego, aby wymusić ich zgodność, lub musisz wprowadzić dodatkowe mechanizmy kontroli.





Krok 3: Planowanie

Na tym etapie znasz już zasoby, podmioty (użytkowników), ruch i przepływy pracy. Teraz musisz przekształcić tę wiedzę w zasady uwierzytelniania i bezpieczeństwa, aby wdrożyć wymaganą architekturę mikrosegmentacji. Jak już wspomnieliśmy, aby uzyskać najlepsze wyniki, należy zastosować połączenie makro- i mikrosegmentacji. Należy pamiętać, że w większości scenariuszy w środowiskach zastanych ograniczeniem będzie istniejąca architektura.

W przypadku makrosegmentacji istnieje wiele opcji, takich jak kanały VLAN, VRF, SPB VPN, VXLAN lub GRE oraz funkcje specjalne, takie jak prywatna sieć VLAN. Każdy z nich ma swoje wady i zalety oraz może być przydatny w różnych sytuacjach. W przypadku mikrosegmentacji musisz wiedzieć, jakie zasady należy uwzględnić w profilu każdego typu użytkownika lub urządzenia. Na koniec musisz zdefiniować sposób przypisywania użytkowników i urządzeń do odpowiedniego segmentu i zasad. Sprowadza się to do uwierzytelniania lub klasyfikacji, która może obejmować identyfikację urządzeń.

Najlepiej byłoby zainwestować w technologię (segmentację definiowaną programowo) umożliwiającą tworzenie elastycznych zasad uwierzytelniania, dzięki czemu można łatwo aktualizować profile sieciowe.

Sugerujemy zaprojektowanie przepływu uwierzytelniania w następującej kolejności:

1. Uwierzytelnianie za pomocą certyfikatów 802.1x przy użyciu serwera RADIUS. Uwierzytelnianie generuje rekord uwierzytelniania. Są to informacje, które można udostępniać zaporom sieciowym.
2. Jeśli nie możesz uwierzytelnić urządzenia za pomocą certyfikatów 802.1x, spróbuj zastosować uwierzytelnianie MAC. Uwierzytelnianie MAC nie jest tak bezpieczne jak przy użyciu 802.1x, ale jest lepsze niż całkowity brak uwierzytelniania. Używaj go do czasu, gdy przejście na 802.1x będzie możliwe.

3. Jeśli nie zostanie uzyskany żaden profil, możesz spróbować metody „odcisków palców”, których możesz również użyć do przypisania do segmentu profilu i zasad. Nie spowoduje to wygenerowania rekordu uwierzytelniania ani księgowania, ale jest rejestrowane w bazie danych spisu urządzeń IoT.

4. Na koniec możesz ustawić domyślną opcję „przechwytyj wszystkie” na wypadek, gdy nie uda się uzyskać żadnego profilu lub każdy inny sposób zawiedzie. Na wczesnych etapach nadal będzie konieczne przypisanie urządzenia do profilu, który będzie prowadził do tego samego segmentu i zasad oraz zarejestruje urządzenie w bazie danych spisu.

Ten przepływ powinno się zorganizować w elastyczny sposób, umożliwiający adaptację w miarę postępów. Można na przykład najpierw wyeliminować uwierzytelnianie MAC i dodać je później, po uzyskaniu listy adresów MAC z raportu z inwentaryzacji. W miarę udoskonalania procesu można na przykład zmienić segment i zasady powiązane z profilem domyślnym na bardzo restrykcyjne, które umożliwiają dostęp tylko do ufortyfikowanej stacji bazowej.

Można także udostępnić rolę urządzenia zaporze, aby zasady zapory mogły być oparte na roli urządzenia, a nie tylko na adresie podsieci/IP. Zalety tej integracji są dwojakie. Po pierwsze, zaporę może zastosować szczegółowe zasady wobec tych urządzeń IoT. Po drugie, zasady zapory są teraz oparte na użytkownikach lub rolach, a więc nie są już powiązane z podsiecią lub adresem IP, co umożliwia przyszłe przeprojektowanie i ponowną segmentację sieci.

Proces ten będzie miał charakter iteracyjny i będzie trzeba go poprawiać, dostrajać i udoskonalać w miarę nabywania doświadczenia w korzystaniu z uwierzytelniania i segmentacji.



Krok 4: Symulacja

Bez względu na to, ile zaplanujesz, jest mało prawdopodobne, że uda Ci się zrealizować plan za pierwszym razem. Każdy błąd w projekcie schematu uwierzytelniania, jakiegokolwiek pominięcie w „liście zezwoleń” strategii bezpieczeństwa spowoduje szkody dla procesu biznesowego. Konieczne będzie zastosowanie zasad uwierzytelniania i dostępu w trybie awaryjnym. Oznacza to, że urządzenia i użytkownicy, których uwierzytelnienie się nie powiedzie, nadal będą dozwolone w sieci, a nieoczekiwany ruch będzie nadal dozwolony. Ale wszystko będzie rejestrowane, a rejestry umożliwią udoskonalenie schematów uwierzytelniania i zasad.

Krok 5: Egzekwowanie

Po pewnym dostrojeniu przestaną się zdarzać niepowodzenia uwierzytelniania ani odmowy legalnych przepływów. Następnie można zastosować zasady „awaryjnego otwierania” do „awaryjnego zamykania”, co oznacza, że nieuczciwe urządzenia zostaną zablokowane, a nieoczekiwane przepływy zostaną odrzucone.

Co oczywiste, nadal trzeba będzie monitorować wszelkie nieoczekiwane urządzenia i przepływy ruchu — w razie potrzeby powtarzając cały cykl.



Jeszcze jedna rzecz

W ramach ciągłego monitorowania, rejestrowania i kwarantanny zalecamy również inwestycję w zewnętrzny system wykrywania włamań (IDS). Chociaż istnieje szereg ataków typu rozproszona odmowa usługi (Distributed Denial of Service, DDoS), które można zidentyfikować bezpośrednio przez sam przełącznik, zewnętrzny IDS może również wykryć szerszy zakres ataków, takich jak wirusy lub inne anomalie. Być może pamiętasz, że przed kilku laty kilka kamer do monitoringu wideo zostało zainfekowanych złośliwym oprogramowaniem Mirai, albo skoordynowany atak tych urządzeń na globalne serwery DNS, który wpłynął na usługi takie jak Twitter, Spotify czy Paypal. Takich ataków nie mogą wykryć Twoje przełączniki, ale dedykowany IDS z pewnością to robi.

Po wykryciu ataku system IDS poinformuje system zarządzania siecią (NMS) o adresach IP urządzeń, których dotyczy problem. W idealnym przypadku system NMS byłby w stanie zlokalizować te urządzenia w swojej bazie danych i zmienić ich profile na „rolę kwarantanny”.

„Rola kwarantanny” to bardzo restrykcyjna rola, która zwykle umożliwia komunikację tylko z ufortyfikowaną stacją bazową, aby możliwe było naprawienie urządzenia, na przykład poprzez ustawienie silnego hasła lub aktualizację oprogramowania firmowego.

Dlaczego warto wybrać ALE?

Rozwiązania w technologii [Digital Age Networking](#) stworzonej przez Alcatel-Lucent Enterprise obejmują solidną i elastyczną segmentację zdefiniowaną programowo z dynamicznymi zasadami DPI NAC, które umożliwiają stopniową ewolucję w kierunku architektury Zero Trust.

Digital Age Networking to projekt firmy Alcatel-Lucent Enterprise, który umożliwia przedsiębiorstwom i organizacjom wejście w erę cyfrową i rozwój biznesów cyfrowych. DAC opiera się na trzech filarach:

- [Sieć autonomiczna](#), która łatwo, automatycznie i bezpiecznie łączy ludzi, procesy, aplikacje i obiekty. Sieć autonomiczna ALE opiera się na usprawnionym portfolio wraz z prawdziwie ujednoliconą platformą zarządzania, zapewniającą wspólne zasady bezpieczeństwa w naszej sieci LAN i WLAN. Sieć autonomiczna zapewnia również elastyczność wdrażania w pomieszczeniach, na zewnątrz i w środowiskach przemysłowych. Zarządzanie siecią może być realizowane lokalnie, w chmurze lub w środowisku hybrydowym, w zależności od preferencji klienta.
- [Bezpieczne i wydajne wdrażanie urządzeń IoT](#): segmentacja utrzymuje urządzenia w dedykowanych segmentach i minimalizuje ryzyko naruszenia bezpieczeństwa urządzenia i sieci. Segmentacja Internetu przedmiotów może pomóc firmom w łatwy i automatyczny sposób stwierdzić, czy urządzenie zachowuje się prawidłowo, oraz pomóc w utrzymaniu bezpieczeństwa sieci.
- [Innowacje biznesowe dzięki automatyzacji przepływu pracy](#): integracja wskaźników użytkowników, aplikacji i IoT w czasie rzeczywistym, z wykorzystaniem danych geolokalizacyjnych w usłudze zarządzania platformami do współpracy, upraszcza tworzenie i wdrażanie nowych zautomatyzowanych procedur biznesowych i usług cyfrowych, w tym powiadamianie administratorów sieci i bezpieczeństwa o wszelkich naruszeniach.

Czy posiadasz narzędzie do tworzenia spisu urządzeń / urządzeń IoT? Czy posiadasz narzędzie, które pozwala monitorować przepływy aplikacji? Czy obecne przełączniki i punkty dostępu bezprzewodowego są gotowe do segmentacji zdefiniowanej programowo? Jeśli obecnie nie posiadasz tych narzędzi, [skontaktuj się z nami](#), a my pomożemy Ci dotrzeć do celu.





Co wiemy na pewno

Podsumujmy kilka kluczowych wniosków:

- Aby uzyskać naprawdę wydajną architekturę ZTA, musisz stosować zarówno makro-, jak i mikrosegmentację
- Wdrażanie architektury ZTA składa się z pięciu kroków: monitorowania, zatwierdzania i oceny, planowania, symulacji i egzekwowania
- Architektura ZTA oparta na mikrosegmentacji ma trzy filary: uwierzytelnianie, przy zastosowaniu złotego standardu 802.1x EAP-TLS; zróżnicowane zasady związane z rolą użytkownika lub urządzenia, które wywodzą się z zasady jak najmniejszych przywilejów; oraz ciągłe monitorowanie i kwarantanna
- W środowiskach hybrydowych i mobilnych mikrosegmentacja musi być zdefiniowana programowo, co oznacza, że musi być dynamiczna i oparta na zasadach, a nie statycznie zdefiniowana, gdyż w przeciwnym razie byłaby niepraktyczna

Migracja do architektury ZTA poprzez mikrosegmentację jest procesem i jest mało prawdopodobne, aby znacznych rozmiarów firma osiągnęła cel w jednym cyklu odświeżania. Jednak w każdym cyklu odświeżania, przeprojektowywania lub ciągłego doskonalenia można zbliżyć się do tego celu, pod warunkiem zastosowania odpowiedniej infrastruktury i projektu.

Alcatel-Lucent Enterprise angażuje się w opracowywanie technologii i rozwiązań sieciowych, które pomagają organizacjom realizować swój potencjał biznesowy poprzez transformację cyfrową.

