NSC NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA	Narodowy Standard Cyberbezpieczeństwa		
Nazwa standardu	Symbol	Wersja	Data wydania
ARCHITEKTURA BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH W MODELU „ZERO ZAUFANIA”	NSC 800-207	1.0	07/09/2021

Architektura bezpieczeństwa systemów informatycznych w modelu „Zero zaufania”

PEŁNOMOCNIK RZĄDU DS. CYBERBEZPIECZEŃSTWA
Warszawa 2021

Niniejsza publikacja, ***Architektura bezpieczeństwa systemów informatycznych w modelu „Zero zaufania”***, opracowana została za zgodą National Institute of Science and Technology (NIST) na podstawie publikacji specjalnej NIST SP 800-207.

Terminologia angielska i akronimy występujące w publikacji zdefiniowane są w dokumencie NSC 7298, ***Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa.***

SPIS TREŚCI

1. WSTĘP

Typowa infrastruktura podmiotów staje się coraz bardziej złożona. Pojedynczy podmiot może obsługiwać kilka sieci wewnętrznych, zdalne biura z własną infrastrukturą lokalną, zdalne i/lub mobilne osoby oraz usługi w chmurze. Złożoność ta wyprzedziła dotychczasowe metody bezpieczeństwa sieci oparte na ochronie granic systemów, ponieważ nie ma w podmiocie jednej, łatwo identyfikowalnej granicy. Wykazano również, że bezpieczeństwo sieci oparte na zabezpieczaniu granicy jest niewystarczające, ponieważ po naruszeniu granicy przez napastników ich dalsze działania nie są utrudniane.

Taka złożoność infrastruktury podmiotów doprowadziła do opracowania nowego modelu cyberbezpieczeństwa, znanego jako „zero zaufania” (*ang. Zero Trust – ZT*). Podejście ZT koncentruje się przede wszystkim na ochronie danych i usług, ale może i powinno zostać rozszerzone na wszystkie aktywa podmiotu (urządzenia, elementy infrastruktury, aplikacje, elementy wirtualne i w chmurze) oraz podmioty (użytkowników końcowych, aplikacje i inne podmioty niebędące ludźmi, które zwracają się do zasobów o informacje). W całym niniejszym dokumencie stosowany będzie termin "podmiot", chyba że część ta odnosi się bezpośrednio do ludzkiego użytkownika końcowego, w którym zwrot "użytkownik" będzie konkretnie używany zamiast bardziej ogólnego terminu "podmiot". Zwrot podmiot będzie występował, zależnie od kontekstu, raz jako rodzaj obiektu uzyskującego dostęp do zasobów, a raz jako organizacja eksploatująca system informatyczny. Modele zabezpieczeń "zero zaufania" zakładają, że napastnik jest obecny w środowisku oraz, że środowisko będące własnością podmiotu nie różni się lub nie jest bardziej wiarygodne od każdego środowiska niebędącego własnością podmiotu. W tym nowym paradygmacie podmiot nie może zakładać domniemanego zaufania oraz musi stale analizować i oceniać ryzyka dla swoich aktywów i funkcji biznesowych, a następnie wprowadzać zabezpieczenia w celu ograniczania tych zagrożeń. W warunkach braku zaufania ochrona ta zazwyczaj polega na ograniczeniu do minimum dostępu do zasobów (takich jak dane i zasoby obliczeniowe oraz aplikacje/usługi) tylko do tych podmiotów i aktywów, które zostały zidentyfikowane jako wymagające dostępu, a także na ciągłym uwierzytelnianiu i autoryzacji tożsamości oraz stanu bezpieczeństwa każdego podmiotu wnioskującego o dostęp.

Architektura „zero zaufania” (*ang. Zero Trust Architecture – ZTA*) jest architekturą cyberbezpieczeństwa podmiotu, która opiera się na zasadach braku zaufania i ma na celu zapobieganie naruszeniom danych i ograniczanie niepożądanego ruchu wewnętrznego. W niniejszej publikacji omówiono ZTA, jej elementy logiczne, możliwe scenariusze wdrożenia oraz zagrożenia. Przedstawiono w niej również ogólny scenariusz postępowania dla podmiotów pragnących przejść na architekturę „zero zaufania” oraz omówiono odpowiednie polityki, które mogą mieć wpływ na architekturę „zero zaufania”.

ZT nie jest pojedynczą architekturą, ale zbiorem zasad przewodnich dla przepływu pracy (*ang. workflow*), projektowania systemu i operacji, które mogą być wykorzystane do poprawy stanu bezpieczeństwa na każdym poziomie kategoryzacji bezpieczeństwa lub poziomie wpływu na organizację [NSC 199][1]. Przejście do ZTA jest procesem odnoszącym się do tego, jak podmiot ocenia ryzyko w swojej misji i nie może być po prostu zrealizowane poprzez hurtowe zastąpienie technologii. Niemniej jednak wiele podmiotów już dziś posiada elementy ZTA w swojej infrastrukturze. Podmioty powinny dążyć do stopniowego wdrażania zasad zerowego zaufania, zmian w procesach i rozwiązań technologicznych, które chronią ich zasoby danych i funkcje biznesowe przez przypadkowe użycie. Większość infrastruktur podmiotów będzie działać w hybrydowym trybie "zero zaufania/ochrona obwodowa", a jednocześnie podmioty te nadal będą inwestować w inicjatywy związane z modernizacją IT i doskonaleniem procesów biznesowych.

Podmioty muszą wdrożyć kompleksowe praktyki w zakresie bezpieczeństwa i odporności informacji, aby zasada "zero zaufania" była skuteczna. Przy zachowaniu równowagi pomiędzy istniejącymi politykami i wytycznymi w zakresie cyberbezpieczeństwa, zarządzaniem tożsamością i dostępem, ciągłym monitorowaniem i najlepszymi praktykami, ZTA może chronić przed powszechnymi zagrożeniami i poprawiać stan bezpieczeństwa podmiotu poprzez zastosowanie podejścia opartego na zarządzaniu ryzykiem.

1.1. HISTORIA WYSIŁKÓW WDRAŻANIA ZASAD ZT W AMERYKAŃSKICH INSTYTUCJACH FEDERALNYCH

Koncepcja "zero za ufania" jest obecna w cyberbezpieczeństwie od czasu, gdy pojęcie "zero zaufania" zostało stworzone. Agencja Systemów Informatycznych Obrony (DISA) i Departament Obrony opublikowały swoje prace nad bardziej bezpieczną strategią podmiotów federalnych nazwaną "czarnym rdzeniem" [BCORE]. „Czarny rdzeń” polegał na przejściu od modelu bezpieczeństwa opartego na granicach do takiego, który skupiał się na bezpieczeństwie poszczególnych transakcji. Prace Jericho Forum w 2004 r. nagłaśniały ideę deperymetryzacji ograniczającej ukryte zaufanie oparte na lokalizacji sieci oraz ograniczenia polegające na pojedynczej, statycznej obronie w dużym segmencie sieci [JERICHO]. Koncepcja deperymetryzacji rozwinęła się i udoskonaliła do większego pojęcia, jakim jest koncepcja zerowego zaufania, które to pojęcie zostało wprowadzone przez Johna Kindervaga[2] i zostało później opisane przez Johna Kindervaga podczas pracy w Forrester[3]. Zerowe zaufanie stało się terminem używanym do opisania różnych rozwiązań w zakresie

[1] Patrz – rozdział Referencje. Dotyczy co całego dokumentu. Nazwy podane w nawiasach kwadratowych [ ] odnoszą się do pozycji wyszczególnionych w rozdziale Referencje.
[2] https://go.forrester.com/blogs/next-generation-access-and-zero-trust/
[3] Wszelkie wzmianki o produktach lub usługach komercyjnych w dokumentach NSC mają charakter wyłącznie informacyjny i nie oznaczają rekomendacji ani wsparcia ze strony rządu.

cyberbezpieczeństwa, które odsunęły bezpieczeństwo od domniemanego zaufania opartego na lokalizacji sieci i zamiast tego skupiły się na ocenie zaufania w odniesieniu do każdej transakcji. Zarówno przemysł prywatny, jak i szkolnictwo wyższe również przeszły tę ewolucję od bezpieczeństwa opartego na zaufaniu perymetrycznym do strategii bezpieczeństwa opartej na zasadach zerowego zaufania.

Od ponad dziesięciu lat agencje federalne są zachęcane do przejścia na bezpieczeństwo oparte na zasadach zerowego zaufania, budując możliwości i polityki takie jak Federalna Ustawa o Modernizacji Bezpieczeństwa Informacji (FISMA), a następnie Ramy Zarządzania Ryzykiem (RMF); Federalne Zarządzanie Tożsamością, Poświadczeniami i Dostępem (FICAM); Zaufane Połączenia Internetowe (TIC); oraz Programy Ciągłej Diagnostyki i Łagodzenia Skutków (CDM). Wszystkie te programy mają na celu ograniczenie dostępu do danych i zasobów tylko uprawnionym stronom. Kiedy programy te zostały uruchomione, były one ograniczone możliwościami technicznymi systemów informatycznych. Polityka bezpieczeństwa była w dużej mierze statyczna i była egzekwowana w dużych "punktach dławienia", które podmiot mógł kontrolować, aby uzyskać jak największy efekt tych działań. W miarę dojrzewania technologii, w celu ograniczenia ekspozycji danych z powodu przejęcia kont przez napastników monitorujących sieć oraz z powodu innych zagrożeń, możliwe staje się ciągłe analizowanie i ocenianie wniosków o dostęp w sposób dynamiczny i ziarnisty, na zasadzie "potrzeby dostępu".

1.2. STRUKTURA DOKUMENTU

Pozostała część dokumentu jest zorganizowana w następujący sposób:

- Rozdział 2 definiuje ZT i ZTA oraz wymienia podstawowe założenia projektowania ZTA na potrzeby podmiotu. Rozdział ten zawiera również listę doktryn projektu ZT.
- Rozdział 3 dokumentuje komponenty logiczne lub bloki konstrukcyjne ZT. Możliwe jest, że unikatowe implementacje składają komponenty ZTA w różny sposób, ale obsługują te same funkcje logiczne.
- W Rozdziale 4 wymieniono kilka możliwych przypadków użycia, w których ZTA może uczynić środowisko podmiotu bezpieczniejszym i mniej podatnym na udaną eksploatację przez atakującego. Przypadki obejmują zdalną pracę pracowników, usługi w chmurze i sieci gości.
- W rozdziale 5 omówiono zagrożenia dla podmiotu korzystającego z ZTA. Wiele z tych zagrożeń jest podobnych do innych rozwiązań architektonicznych, ale mogą wymagać różnych technik łagodzenia ich skutków.
- W Rozdziale 6 omówiono sposób, w jaki założenia ZTA wpisują się w istniejące wytyczne dla podmiotów publicznych i/lub je uzupełniają.

- W Rozdziale 7 przedstawiono punkt wyjścia do przejścia podmiotu (np. ministerstwa) na ZTA. Zawiera on opis ogólnych kroków niezbędnych do planowania i wdrażania aplikacji i infrastruktury podmiotu, które są zgodne z zasadami ZT.

2. PODSTAWY PODEJŚCIA „ZERO ZAUFANIA”

Zerowe zaufanie jest paradygmatem cyberbezpieczeństwa skoncentrowanym na ochronie zasobów i założeniu, że zaufanie nigdy nie jest udzielane w sposób dorozumiany, ale musi być stale oceniane. Architektura Zerowe Zaufanie to kompleksowe podejście do bezpieczeństwa zasobów podmiotu i danych, które obejmuje tożsamość (osób fizycznych i podmiotów niebędących osobami fizycznymi), dane uwierzytelniające, zarządzanie dostępem, operacje, punkty końcowe, środowiska hostingowe i infrastrukturę łączącą. Początkowo należy skoncentrować się na ograniczeniach w odniesieniu do tych zasobów niezbędnych do realizacji misji, które wymagają dostępu i przyznania jedynie minimalnych uprawnień (np. czytanie, pisanie, usuwanie). Tradycyjnie, podmioty (i ogólnie sieci podmiotów) skupiają się na ochronie obwodowej, a podmioty uwierzytelnione otrzymują na stałe autoryzowany dostęp do szerokiego zbioru zasobów w sieci wewnętrznej. W rezultacie, nieautoryzowane przepływy uboczne w obrębie środowiska są jednym z największych wyzwań dla podmiotów publicznych.

Zaufane połączenia internetowe (*ang. Trusted Internet Connections – TIC*) i zapory obwodowe podmiotu zapewniane są przez silne bramy internetowe. Pomaga to blokować napastników z Internetu, ale TIC i zapory obwodowe są mniej przydatne do wykrywania i blokowania ataków z wewnątrz sieci i nie mogą chronić podmiotów poza obrębem przedsiębiorstwa (np. pracowników zdalnych, usług w chmurze, urządzeń brzegowych itp.).

Operacyjna definicja "zero zaufania" i architektury "zero zaufania" jest następująca:

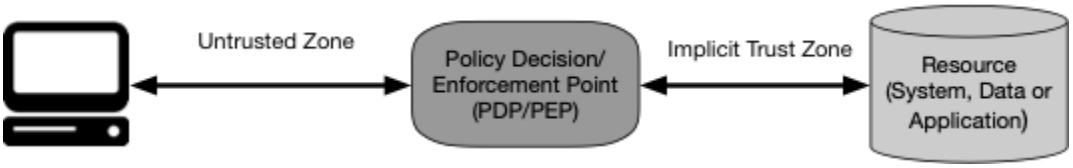
> Zerowe zaufanie (ZT) to zbiór koncepcji i idei mających na celu zapewnienie bezpiecznego dostęp do zasobów niezależnie od ich lokalizacji, przydzielania minimalnych wymaganych uprawnień, ścisłego przestrzegania reguł kontroli dostępu oraz monitorowania całego ruchu sieciowego, również tego z sieci wewnętrznej – domyślnie uznawanego za podejrzany.
>
> Architektura Zerowego Zaufania (ZTA) to plan cyberbezpieczeństwa podmiotu, który wykorzystuje koncepcje zerowego zaufania i obejmuje relacje między komponentami, planowanie przepływu pracy i polityki dostępu. Dlatego też architektura „zero zaufania” jest infrastrukturą sieciową (fizyczną i wirtualną) oraz politykami operacyjnymi, które są stosowane w podmiocie jako produkt planu architektury „zero zaufania”.

Podmiot postanawia przyjąć strategię "zero zaufania" jako swoją podstawową strategię i stworzyć architekturę "zero zaufania" jako plan opracowany z myślą o zasadach "zero zaufania" (patrz sekcja 2.1 poniżej). Plan ten jest następnie wdrażany w celu stworzenia środowiska opartego na zasadzie "zero zaufania" do wykorzystania w tym podmiocie.

Definicja ta koncentruje się na sednie problemu, którym jest zapobieganie nieautoryzowanemu dostępowi do danych i usług w połączeniu z jak najbardziej szczegółowym egzekwowaniem kontroli dostępu. Oznacza to, że upoważnione i zatwierdzone podmioty (połączenie użytkownika, aplikacji (lub usługi) i urządzenia) mogą uzyskać dostęp do danych z wyłączeniem wszystkich innych podmiotów (tj. atakujących). Aby pójść o krok dalej, słowo "dane" można zastąpić słowem "zasób", tak aby ZT i ZTA dotyczyły dostępu do zasobów (np. drukarki, zasobów obliczeniowych, czujników i mechanizmów wykonawczych Internetu Rzeczy (*ang. Internet of Things – IoT*)), a nie tylko dostępu do danych.

W celu zmniejszenia niepewności (ponieważ nie można jej wyeliminować), należy skupić się na uwierzytelnianiu, autoryzacji i zmniejszaniu domyślnych stref zaufania przy jednoczesnym zachowaniu dostępności i minimalizacji czasowych opóźnień w mechanizmach uwierzytelniania. Reguły dostępu są maksymalnie uproszczone, aby wyegzekwować jak najmniej przywilejów potrzebnych do wykonania danej czynności.

W abstrakcyjnym modelu dostępu pokazanym na rysunku 1, podmiot potrzebuje dostępu do zasobów swojej organizacji. Dostęp udzielany jest poprzez punkt zasad decyzji (*ang. policy decision point – PDP*) i odpowiadający mu punkt realizacji zasad (*ang. policy enforcement point – PEP*)[4].



Rysunek 1. Dostęp według zasady "zero zaufania"

System musi upewnić się co do autentyczności wnioskującego o dostęp i ważności wniosku. PDP/PEP wydaje odpowiednią decyzję, aby umożliwić wnioskującemu dostęp do zasobów. Oznacza to, że „zero zaufania” odnosi się do dwóch podstawowych obszarów: uwierzytelniania i autoryzacji. Jaki jest poziom zaufania co do tożsamości uczestnika dla tego unikatowego wniosku? Czy dostęp do zasobu jest dozwolony, biorąc pod uwagę poziom zaufania do tożsamości wnioskującego? Czy urządzenie użyte do zgłoszenia ma odpowiednią klasę bezpieczeństwa? Czy istnieją inne czynniki, które powinny być wzięte pod uwagę i które zmieniają poziom zaufania (np. czas, miejsce pobytu uczestnika, przyznana klasa bezpieczeństwa uczestnika)? Ogólnie rzecz biorąc, podmioty muszą opracować i utrzymać dynamiczne, oparte na ryzyku zasady dostępu do zasobów oraz stworzyć system

[4] Część pojęć zdefiniowanych w OASIS XACML 2.0 https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

zapewniający prawidłowe i spójne egzekwowanie tych zasad w odniesieniu do poszczególnych wniosków o dostęp do zasobów. Oznacza to, że dana organizacja nie powinna polegać na dorozumianej wiarygodności, w przypadku gdy wnioskujący o dostęp osiągnął podstawowy poziom uwierzytelnienia (np. zalogowanie się do zasobu) zakładając, że wszystkie kolejne wnioski o dostęp do zasobów są równie ważne.

Strefa domniemanego zaufania reprezentuje obszar, w którym wszystkie podmioty są zaufane co najmniej do poziomu ostatniej bramki PDP/PEP. Na przykład, należy wziąć pod uwagę model kontroli bezpieczeństwa pasażerów w porcie lotniczym. Wszyscy pasażerowie przechodzą przez punkt kontroli bezpieczeństwa portu lotniczego (PDP/PEP), aby dostać się do bramek wejściowych. Pasażerowie, personel portu lotniczego, załoga samolotu itp. znajdują się na terenie terminalu, a wszystkie osoby uważane są za godne zaufania. W tym modelu strefa domniemanego zaufania jest strefą wejścia na pokład.

PDP/PEP stosuje zestaw kontroli tak, aby cały ruch poza PEP miał wspólny poziom zaufania. PDP/PEP nie może stosować dodatkowych zasad poza swoją lokalizacją w przepływie ruchu. Aby PDP/PEP było jak najbardziej szczegółowe, strefa domniemanego zaufania musi być jak najmniejsza.

Zerowe zaufanie stanowi zbiór zasad i koncepcji dotyczących przybliżania PDP/PEP do zasobów. Ideą jest wyraźne uwierzytelnienie i autoryzacja wszystkich podmiotów, aktywów i przepływów pracy, które składają się na daną organizację.

2.1. ZASADY „ZERO ZAUFANIA”

W wielu definicjach i dyskusjach na temat ZT podkreśla się koncepcję usuwania zabezpieczeń obwodowych o szerokim zasięgu (np. zapór sieciowych w podmiotach). Większość tych definicji nadal jednak w pewien sposób definiuje się w odniesieniu do obwodów (np. mikro-segmentacja lub mikro-obwód; zob. pkt 3.1) jako część funkcjonalnych możliwości ZTA. Poniżej przedstawiono próbę zdefiniowania ZT i ZTA w kategoriach podstawowych doktryn, które powinny być zaangażowane, a nie tego, co jest wykluczone. Te zasady są idealnym celem, choć należy przyznać, że nie wszystkie doktryny mogą być w pełni wdrożone w najczystszej postaci dla danej strategii.

Architektura „zero zaufania” jest projektowana i wdrażana z zachowaniem następujących podstawowych zasad zerowego zaufania:

1. Wszystkie źródła danych i usługi obliczeniowe są uznawane za zasoby. Sieć może składać się z wielu klas urządzeń. Sieć może również zawierać urządzenia o małym zasięgu, które wysyłają dane do agregatorów/przechowalni; oprogramowania jako usługi (SaaS); systemy wysyłające instrukcje do urządzeń wykonawczych i inne funkcje. Ponadto podmiot może podjąć decyzję o zaklasyfikowaniu urządzeń

będących własnością prywatną jako zasobów, jeżeli takie urządzenia mogą uzyskać dostęp do zasobów podmiotu.

2. Cała komunikacja jest zabezpieczona niezależnie od lokalizacji w sieci. Sama lokalizacja w sieci nie oznacza zaufania. Żądania dostępu do zasobów znajdujących się w infrastrukturze sieci należącej do podmiotu (np. w obrębie dotychczasowego obwodu sieci) muszą spełniać te same wymogi bezpieczeństwa, co żądania dostępu i komunikacja z każdej innej sieci niebędącej własnością podmiotu. Innymi słowy, zaufanie nie powinno być przyznawane automatycznie na podstawie tego, że urządzenie znajduje się w infrastrukturze sieci podmiotu. Wszelka komunikacja powinna odbywać się w najbardziej dostępny bezpieczny sposób, chronić poufność i integralność oraz zapewniać uwierzytelnienie źródłowe.
3. Dostęp do poszczególnych zasobów podmiotu jest przyznawany na zasadzie sesji. Zaufanie do wnioskodawcy jest oceniane przed udzieleniem dostępu. Dostęp powinien być również udzielany z najmniejszymi uprawnieniami niezbędnymi do wykonania zadania. Może to oznaczać tylko "jakiś czas temu" w przypadku tej konkretnej transakcji i nie może nastąpić bezpośrednio przed rozpoczęciem sesji lub przeprowadzeniem transakcji z wykorzystaniem danego zasobu. Jednak uwierzytelnienie i autoryzacja do jednego zasobu nie przyznaje automatycznie dostępu do innego zasobu.
4. Dostęp do zasobów jest określany przez dynamiczną zasadę - w tym obserwowalny stan tożsamości klienta, aplikacji/usługi oraz żądającego zasobu - i może obejmować inne atrybuty behawioralne i środowiskowe. Organizacja chroni zasoby poprzez zdefiniowanie, jakie zasoby posiada, kim są jej członkowie (lub możliwość uwierzytelnienia użytkowników ze zrzeszonej społeczności) oraz jakiego dostępu do zasobów potrzebują ci członkowie. W przypadku braku zaufania, tożsamość klienta może obejmować konto użytkownika (lub tożsamość usługi) oraz wszelkie powiązane atrybuty przypisane przez organizację do tego konta lub artefakty służące do uwierzytelniania zautomatyzowanych zadań. Żądanie stanu zasobów może obejmować takie cechy urządzenia, jak zainstalowane wersje oprogramowania, lokalizacja sieci, czas/data żądania, poprzednio obserwowane zachowanie oraz zainstalowane dane uwierzytelniające. Atrybuty behawioralne obejmują między innymi automatyczną analizę obiektu, analizę urządzenia i mierzone odchylenia od obserwowanych wzorców użytkowania. Zasady to zbiór reguł dostępu opartych na atrybutach, które organizacja przypisuje podmiotowi, aktywowi danych lub aplikacji. Atrybuty środowiskowe mogą obejmować takie czynniki jak lokalizacja w sieci, czas, zgłaszane aktywne ataki itp. Te reguły i atrybuty są oparte na potrzebach procesu biznesowego i akceptowalnym poziomie ryzyka. Zasady dostępu do zasobów

i zezwolenia na działania mogą się różnić w zależności od wrażliwości zasobów/danych. W celu ograniczenia zarówno widoczności, jak i dostępności stosuje się zasady dotyczące najmniejszych uprawnień.

5. Podmiot monitoruje i mierzy integralność i bezpieczeństwo wszystkich posiadanych i powiązanych zasobów. Żaden składnik aktywów nie jest z natury rzeczy godny zaufania. Podmiot ocenia klasę bezpieczeństwa składnika aktywów podczas oceny wniosku o udostępnienie zasobów. Podmiot wdrażający ZTA powinien ustanowić system ciągłej diagnostyki i ograniczania zagrożeń (*ang. continuous diagnostics and mitigation* – CDM) lub podobny system do monitorowania stanu urządzeń i aplikacji oraz w razie potrzeby stosować poprawki i uaktualnienia. Aktywa, co do których stwierdzono, że zostały zinfiltrowane, mają znane podatności lub nie są zarządzane przez podmiot, mogą być traktowane inaczej (łącznie z odmową wszystkich połączeń z zasobami podmiotu) niż urządzenia będące własnością podmiotu lub z nim związane w inny sposób, które uznaje się za znajdujące się w najbardziej bezpiecznym stanie. Może mieć to również zastosowanie do urządzeń powiązanych (np. urządzeń będących własnością prywatną), które mogą mieć dostęp do niektórych zasobów, ale nie do wszystkich. Wymaga to również wprowadzenia solidnego systemu monitorowania i raportowania, który zapewni wiarygodne dane na temat aktualnego stanu zasobów podmiotu.
6. Wszelkie uwierzytelnianie i autoryzacja zasobów są dynamiczne i ściśle egzekwowane przed uzyskaniem dostępu. Jest to ciągły cykl uzyskiwania dostępu, skanowania i oceny zagrożeń, dostosowywania i ciągłej oceny zaufania do bieżącej komunikacji. Od podmiotu wdrażającego ZTA oczekuje się posiadania systemów zarządzania tożsamością, wiarygodnością i dostępem (*ang. Identity, Credential, and Access Management –ICAM*) oraz zarządzania zasobami. Obejmuje to wykorzystanie uwierzytelniania wielskładnikowego (*ang. multifactor authentication* – MFA) w celu uzyskania dostępu do niektórych lub wszystkich zasobów podmiotu. Ciągłe monitorowanie z ewentualnym ponownym uwierzytelnieniem i autoryzacją odbywa się w trakcie transakcji z użytkownikami, zgodnie z określonymi i egzekwowanymi zasadami (np. w oparciu o czas, nowe żądane zasoby, modyfikacje zasobów, wykryte anomalie podmiotowe), które dążą do osiągnięcia równowagi między bezpieczeństwem, dostępnością, użytecznością i efektywnością kosztową.
7. Podmiot gromadzi jak najwięcej informacji o aktualnym stanie aktywów, infrastruktury sieciowej i komunikacji oraz wykorzystuje je do poprawy swojego poziomu bezpieczeństwa. Podmiot powinien gromadzić dane na temat klasy bezpieczeństwa aktywów, ruchu w sieci i wniosków o dostęp, przetwarzać te dane i wykorzystywać wszelkie uzyskane informacje do poprawy tworzenia i egzekwowania

ustanowionych zasad. Dane te mogą być również wykorzystywane w celu zapewnienia kontekstu dla wniosków o dostęp składanych przez wnioskujących (zob. sekcja 3.3.1).

Powyższe doktryny próbują być agnostyczne technologicznie. Na przykład, "identyfikacja użytkownika (ID)" może obejmować kilka czynników, takich jak nazwa użytkownika/hasło, certyfikaty i hasło jednorazowe. Te zasady mają zastosowanie do pracy wykonywanej w ramach organizacji lub we współpracy z jedną lub kilkoma organizacjami partnerskimi, a nie do anonimowych, publicznych lub konsumenckich procesów biznesowych. Organizacja nie może narzucać zasad wewnętrznych podmiotom zewnętrznym (np. klientom lub ogólnym użytkownikom Internetu), ale może być w stanie wdrożyć niektóre zasady oparte na ZT w stosunku do użytkowników nieprowadzących działalności gospodarczej, którzy mają szczególne relacje z organizacją (np. zarejestrowani klienci, osoby zależne od pracowników itp.).

2.2. „ZERO ZAUFANIA” Z PUNKTU WIDZENIA SIECI

Dla każdej organizacji, która wykorzystuje ZTA w planowaniu i wdrażaniu sieci, istnieją pewne podstawowe założenia dotyczące łączności sieciowej. Niektóre z tych założeń odnoszą się do infrastruktury sieciowej należącej do danej organizacji, a inne do zasobów organizacji działających na infrastrukturze sieciowej niebędącej jej własnością (np. publiczne sieci Wi-Fi lub publiczni dostawcy usług w chmurze). Założenia te są wykorzystywane przy tworzeniu ZTA. Sieć w podmiocie wdrażającym ZTA powinna być rozwijana zgodnie z przedstawionymi powyżej założeniami ZTA oraz z następującymi założeniami:

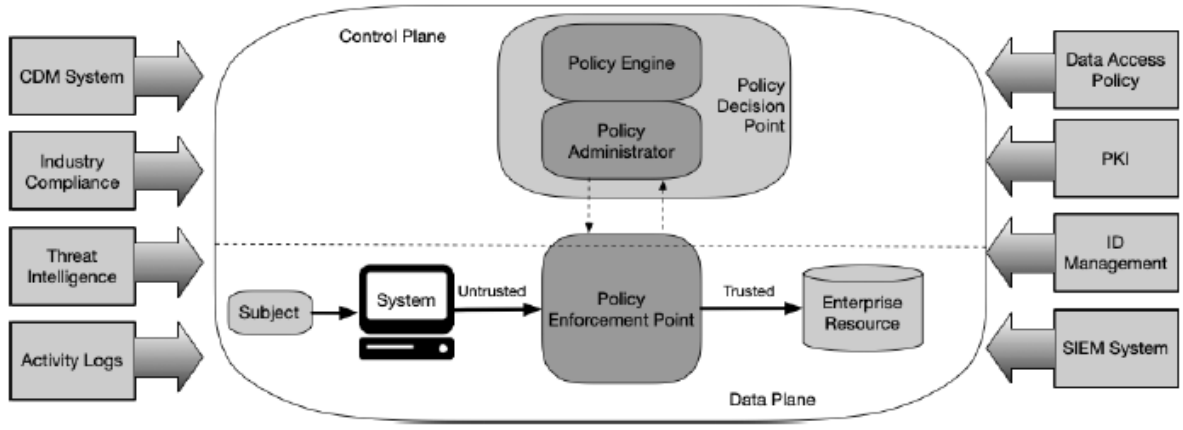
1. Cała sieć prywatna organizacji nie jest uważana za domniemaną strefę zaufania. Aktywa powinny zawsze zachowywać się tak, jakby napastnik był obecny w wewnętrznej sieci organizacji, a komunikacja powinna odbywać się w najbezpieczniejszy dostępny sposób (patrz punkt 2.1.2 powyżej). Wiąże się to z takimi działaniami, jak uwierzytelnianie wszystkich połączeń i szyfrowanie całego ruchu.
2. Urządzenia w sieci mogą nie być własnością organizacji lub mogą nie być konfigurowane przez organizację. Odwiedzający lub zakontraktowane usługi mogą obejmować aktywa niebędące własnością organizacji, ale które do pełnienia swojej roli potrzebują dostępu do sieci organizacji. Obejmuje to zasady „przynieś własne urządzenie” (*ang. bring-your-own-device - BYOD*), które umożliwiają podmiotom korzystanie z urządzeń niebędących ich własnością w celu uzyskania dostępu do zasobów podmiotu.
3. Żaden zasób nie jest z natury rzeczy godny zaufania. Zanim wniosek o dostęp do zasobów organizacji zostanie przyjęty (podobnie jak w przypadku zasobów

i podmiotów, o których mowa w punkcie 2.1.6 powyżej), każdy zasób musi zostać poddany ocenie przez PEP. Ocena ta powinna być przeprowadzana nieprzerwanie tak długo, jak długo trwa sesja. Urządzenia będące własnością organizacji mogą posiadać artefakty, które umożliwiają uwierzytelnienie i zapewniają poziom zaufania wyższy niż ten sam wniosek pochodzący z urządzeń niebędących własnością organizacji. Same dane uwierzytelniające nie wystarczą do uwierzytelnienia urządzenia do zasobów organizacji.

4. Nie wszystkie zasoby organizacji znajdują się w infrastrukturze będącej jej własnością. Zasoby te obejmują zdalne podmioty organizacji oraz usługi w chmurze. Zasoby należące do organizacji lub zarządzane przez organizację mogą wymagać wykorzystania lokalnej (tj. nie należącej do organizacji) sieci do podstawowych usług łączności i usług sieciowych (np. usługi DNS).
5. Zdalne podmioty i aktywa organizacji nie mogą mieć pełnego zaufania do swojego połączenia z siecią lokalną. Zdalne podmioty powinny założyć, że sieć lokalna (tj. sieć niebędąca własnością organizacji) jest wroga. Aktywa powinny zakładać, że cały ruch jest monitorowany i potencjalnie modyfikowany. Wszystkie wnioski o połączenie powinny być uwierzytelnione i autoryzowane, a cała komunikacja powinna odbywać się w możliwie najbezpieczniejszy sposób (tj. zapewniać poufność, ochronę integralności i uwierzytelnianie źródła). Patrz założenia ZTA powyżej.
6. Aktywa i przepływy dokumentów pomiędzy infrastrukturą organizacji i infrastrukturą niebędąca własnością organizacji powinny mieć spójne zasady bezpieczeństwa. Aktywa i obieg dokumentów powinny zachować swoją klasę w zakresie bezpieczeństwa podczas przenoszenia się do lub z infrastruktury będącej własnością organizacji. Obejmuje to urządzenia przenoszące się z sieci organizacji do innych sieci (tj. użytkowników zdalnych). Obejmuje to również obciążenia związane z migracją z centrów danych znajdujących się w lokalizacji organizacji do instancji chmury poza organizacją.

3. LOGICZNE KOMPONENTY ARCHITEKTURY „ZERO ZAUFANIA”

Istnieje wiele elementów logicznych, które składają się na wdrożenie ZTA w organizacji. Komponenty te mogą być obsługiwane jako usługa w siedzibie lub poprzez usługę w chmurze. Model koncepcyjny przedstawiony na rysunku 2 pokazuje podstawowe zależności między komponentami i ich interakcjami. Należy zauważyć, że jest to idealny model pokazujący logiczne komponenty i ich interakcje. Punkt decyzyjny polityki (PDP) z rysunku 1, jest podzielony na dwa logiczne komponenty (zdefiniowane na rysunku 2): silnik zasad (*ang. Policy Engine*) i administratora zasad (*ang. Policy Administrator*). Komponenty logiczne ZTA wykorzystują do komunikacji oddzielną płaszczyznę sterowania, podczas gdy dane aplikacji są przekazywane na płaszczyźnie danych (patrz punkt 3.4).



Rysunek 2. Podstawowe komponenty logiczne architektury 'Zero Zaufania"[5]

Opis komponentów:

- Silnik zasad (PE): Komponent ten jest odpowiedzialny za podjęcie ostatecznej decyzji o przyznaniu dostępu do zasobów dla danego podmiotu. Mechanizm stałego rozwoju wykorzystuje politykę organizacji, jak również dane ze źródeł zewnętrznych (np. systemów CDM, służb wywiadowczych ds. zagrożeń opisanych poniżej) jako dane wejściowe do algorytmu zaufania (więcej szczegółów w sekcji 3.3) w celu udzielenia, odmowy lub odwołania dostępu do zasobu. PE jest połączony z komponentem dotyczącym administratora polityki (PA). Mechanizm zasad podejmuje i rejestruje decyzję (zatwierdzoną lub odrzuconą), a administrator zasad wykonuje decyzję.
- Administrator zasad (PA): Komponent ten jest odpowiedzialny za ustanowienie lub zamknięcie ścieżki komunikacyjnej między podmiotem, a zasobem (poprzez polecenia dla odpowiednich PEP). W celu uzyskania przez klienta dostępu do zasobów organizacji, generuje on specyficzny dla danej sesji sposób uwierzytelnienia w postaci

[5] Rozwinięcie angielskich nazw znajduje się w tekście w akapicie: Opis komponentów.

tokenu uwierzytelniania lub poświadczenie tożsamości. Jest on ściśle powiązany z PE i opiera się na jego decyzji w zakresie ostatecznego zezwolenia na sesję lub odmowie jej przeprowadzenia. Jeżeli sesja jest autoryzowana, a żądanie uwierzytelnione, PE konfiguruje PEP, aby umożliwić rozpoczęcie sesji. Jeśli sesja zostanie odrzucona (lub poprzednie zatwierdzenie zostanie odrzucone), PA sygnalizuje PEP, aby zamknąć połączenie. Niektóre implementacje mogą traktować PE i PA jako jedną usługę; tutaj jest ona podzielona na dwa elementy logiczne. PA komunikuje się z PEP podczas tworzenia ścieżki komunikacyjnej. Komunikacja ta odbywa się poprzez płaszczyznę sterowania.

- Punkt egzekwowania zasad (PEP): System ten jest odpowiedzialny za włączanie, monitorowanie i ostatecznie kończenie połączeń między podmiotem, a zasobami organizacji. PEP komunikuje się z PA w celu przekazywania wniosków i/lub otrzymywania od niego aktualizacji zasad. Jest to pojedynczy komponent logiczny w ZTA, ale może być podzielony na dwa różne komponenty: klient (np. agent na laptopie) i strona zasobów (np. komponent bramki przed zasobem, który kontroluje dostęp) lub pojedynczy komponent portalu, który działa jako strażnik ścieżek komunikacyjnych. Poza PEP jest to strefa zaufania (patrz Sekcja 2).

Oprócz podstawowych komponentów w organizacji wdrażającej ZTA, kilka źródeł danych dostarcza danych wejściowych określających sposób funkcjonowania PE przy podejmowaniu decyzji o dostępie. Należą do nich zarówno lokalne źródła danych, jak i zewnętrzne źródła danych (tj. niekontrolowane lub nietworzone przez organizacje). Mogą one obejmować:

- System ciągłej diagnostyki i łagodzenia skutków (*ang. Continuous diagnostics and mitigation - CDM*): Gromadzi on informacje o aktualnym stanie aktywów organizacji i stosuje aktualizacje konfiguracji i składników oprogramowania. System CDM klasy korporacyjnej dostarcza silnikowi zasad informacje o składającym żądanie dostępu do składnika aktywów, takie jak informacje o tym, czy działa on z odpowiednim, poprawionym systemem operacyjnym (OS), o integralności zatwierdzonych przez organizację komponentów oprogramowania lub o obecności niezatwierdzonych komponentów oraz o tym, czy składnik aktywów posiada znane podatności. Systemy CDM są również odpowiedzialne za identyfikację i potencjalne egzekwowanie podzbioru zasad dotyczących urządzeń nie będących własnością organizacji, działających w ramach infrastruktury organizacji.
- System zgodności branżowej (*ang. Industry compliance system*): Zapewnia to, że organizacja pozostaje w zgodzie z każdym systemem regulacyjnym, do którego musi się stosować (np. wymagania bezpieczeństwa dla podmiotów publicznych, wymagania bezpieczeństwa informacji w służbie zdrowia lub branży finansowej).

Obejmuje to wszystkie zasady, które organizacja opracowuje w celu zapewnienia zgodności z przepisami.

- Kanał(y) wywiadowczy(e) dotyczący(e) zagrożeń (*ang. Threat intelligence*): Zapewnia to informacje ze źródeł wewnętrznych lub zewnętrznych, które pomagają w podejmowaniu decyzji dotyczących dostępu do danych. Mogą to być różnorodne usługi, które pobierają dane z wewnętrznych lub zewnętrznych źródeł i dostarczają informacji o nowo wykrytych atakach lub podatnościach. Obejmuje to również nowo odkryte wady w oprogramowaniu, nowo zidentyfikowane złośliwe oprogramowanie oraz zgłoszone ataki na inne aktywa, do których silnik zasad będzie chciał odmówić dostępu.
- Dzienniki aktywności sieci i systemu (*ang. Network and system activity logs*): Ten system korporacyjny agreguje dzienniki aktywów, ruch sieciowy, działania związane z dostępem do zasobów i inne zdarzenia, które dostarczają informacji zwrotnych w czasie rzeczywistym (lub prawie rzeczywistym) na temat klasy bezpieczeństwa systemów informatycznych organizacji.
- Zasady dostępu do danych (*ang. Data access policies*): Są to atrybuty, reguły i zasady dotyczące dostępu do zasobów organizacji. Zestaw tych reguł może być zakodowany na stałe (poprzez interfejs zarządzania) lub dynamicznie generowany przez silnik zasad. Zasady te stanowią punkt wyjścia do autoryzacji dostępu do zasobów, ponieważ zapewniają podstawowe uprawnienia dostępu do kont i aplikacji/usług w organizacji. Zasady te powinny być oparte na zdefiniowanych rolach i potrzebach organizacji.
- Infrastruktura klucza publicznego organizacji (*ang. public key infrastructure - PKI*): System ten jest odpowiedzialny za generowanie i logowanie certyfikatów wydawanych przez organizację dla zasobów, podmiotów, usług i aplikacji. Obejmuje on również ekosystem globalnego organu certyfikacyjnego oraz rządowy PKI , który może, ale nie musi być zintegrowany z PKI organizacji. Może to być również PKI, który nie jest zbudowany na bazie certyfikatów X.509.
- System zarządzania identyfikatorami (*ang. ID management system*): Jest to system odpowiedzialny za tworzenie, przechowywanie i zarządzanie kontami użytkowników i rekordami tożsamości (np. lekki serwer protokołu dostępu do katalogów (LDAP)). System ten zawiera niezbędne informacje tematyczne (np. nazwę, adres e-mail, certyfikaty) oraz inne cechy organizacji, takie jak role, atrybuty dostępu i przypisane aktywa. System ten często wykorzystuje inne systemy (takie jak PKI) do tworzenia artefaktów związanych z kontami użytkowników. System ten może być częścią

większej społeczności i może obejmować pracowników spoza organizacji lub powiązania z aktywami spoza organizacji w celu współpracy.

- System bezpieczeństwa informacji i zarządzania zdarzeniami (*ang. Security information and event management - SIEM*): System ten gromadzi informacje istotne z punktu widzenia bezpieczeństwa w celu ich późniejszej analizy. Dane te są następnie wykorzystywane do udoskonalania zasad i ostrzegania przed możliwymi atakami na aktywa organizacji.

3.1. WARIANTY PODEJŚCIA W RAMACH ARCHITEKTURY „ZERO ZAUFANIA”

Istnieje kilka sposobów, w jaki organizacja może wprowadzić ZTA w organizacji stojących przed nią zadań. Podejścia te różnią się między sobą pod względem zastosowanych komponentów oraz głównego źródła zasad dla danej organizacji. Każde podejście realizuje wszystkie założenia ZT (zob. sekcja 2.1), ale może wykorzystywać jeden lub kilka komponentów jako główny sterownik stosowanych zasad. Pełne rozwiązanie ZT będzie obejmowało elementy wszystkich trzech podejść. Podejścia te obejmują rozszerzone zarządzanie tożsamością, logiczną mikro-segmentację oraz segmentację opartą na sieci.

Niektóre podejścia nadają się do stosowania w danych przypadkach bardziej niż inne. Organizacja dążąca do opracowania ZTA może stwierdzić, że wybrany przez nią przypadek zastosowania i istniejące zasady wskazują na jedno podejście w porównaniu z innymi. Nie oznacza to, że inne podejścia nie będą działać, ale te inne podejścia mogą być trudniejsze do wdrożenia i mogą wymagać bardziej fundamentalnych zmian w sposobie, w jaki organizacja obecnie prowadzi przepływy biznesowe.

3.1.1. ZTA STOSUJĄCA ROZSZERZONE ZARZĄDZANIE TOŻSAMOŚCIĄ

Rozszerzone podejście do zarządzania tożsamością przy opracowywaniu ZTA wykorzystuje tożsamość podmiotów jako kluczowy element tworzenia zasad. Gdyby nie podmioty wnioskujące o dostęp do zasobów przedsiębiorstwa, nie byłoby potrzeby tworzenia zasad dostępu. W przypadku tego podejścia, zasady dostępu do zasobów organizacji opierają się na tożsamości i przypisanych atrybutach. Podstawowe wymaganie dotyczące dostępu do zasobów opiera się na uprawnieniach dostępu przyznanych danemu podmiotowi. Inne czynniki, takie jak zastosowane urządzenie, stan aktywów i czynniki środowiskowe mogą zmienić ostateczne wyznaczenie poziomu zaufania (i ostateczne upoważnienie dostępu) lub w pewien sposób dostosować wynik, np. przyznając tylko częściowy dostęp do danego źródła danych w oparciu o lokalizację sieci. Poszczególne zasoby lub komponenty PEP chroniące dany zasób muszą mieć możliwość przekazywania wniosków do usługi PE lub uwierzytelniania podmiotu i zatwierdzania wniosku przed udzieleniem dostępu.

W przypadku organizacji często stosuje się podejścia oparte na rozszerzonym zarządzaniu tożsamością, wykorzystujące model sieci otwartej lub sieci organizacji z dostępem dla gości, często z urządzeniami w sieci nie będącymi częścią organizacji (np. przypadek zastosowania opisany w sekcji 4.3 poniżej). Dostęp do sieci jest początkowo przyznawany do wszystkich aktywów, ale dostęp do zasobów organizacji jest ograniczony do tożsamości z odpowiednimi uprawnieniami dostępu. Przyznanie podstawowego dostępu do sieci ma pewną wadę, ponieważ podmioty złośliwe mogą nadal próbować przeprowadzić rozpoznanie sieci lub wykorzystać sieć do przeprowadzenia ataków typu Denial of Service, zarówno wewnętrznych, jak i przeciwko osobom trzecim. Organizacje nadal muszą monitorować takie zachowanie i reagować na nie, zanim wpłynie ono na organizację pracy.

Podejście oparte na tożsamości dobrze współgra z modelem portalu zasobów (zob. sekcja 3.2.3), ponieważ tożsamość i status urządzenia dostarczają dodatkowych danych pomocniczych do podejmowania decyzji. W zależności od obowiązujących zasad działają również inne modele. Podejścia oparte na tożsamości działają również dobrze w przypadku organizacji, które korzystają z aplikacji/usług opartych na chmurze, które mogą nie pozwalać na wykorzystanie należących do przedsiębiorstwa lub obsługiwanych przez nie komponentów bezpieczeństwa ZT (takich jak wiele ofert SaaS). Przedsiębiorstwo może wykorzystywać tożsamość wnioskodawców do tworzenia i egzekwowania zasad na tych platformach.

3.1.2. ZTA WYKORZYSTUJĄCA MIKRO-SEGMENTACJĘ

Organizacja może zdecydować się na wdrożenie ZTA w oparciu o umieszczenie indywidualnych lub poszczególnych grup zasobów w unikatowym segmencie sieci chronionym przez komponent bezpieczeństwa bramki. W takim podejściu organizacja umieszcza urządzenia infrastrukturalne, takie jak inteligentne przełączniki (lub routery) lub zapory nowej generacji (*ang. next generation firewall - NGFW*) lub urządzenia bramowe specjalnego przeznaczenia, które pełnią rolę PEP-ów chroniących każdy zasób lub małą grupę powiązanych zasobów. Alternatywnie (lub dodatkowo) organizacja może zdecydować się na wdrożenie mikro-segmentacji opartej na hostach przy użyciu agentów programowych (zob. sekcja 3.2.1) lub zapór sieciowych na aktywach punktów końcowych. Urządzenia bramowe dynamicznie przyznają dostęp dla indywidualnych żądań klienta, aktywów lub usług.
W zależności od modelu, bramka może być jedynym komponentem PEP lub częścią wieloskładnikowego PEP składającego się z bramy i agenta po stronie klienta (patrz Sekcja 3.2.1).

Podejście to ma zastosowanie w różnych przypadkach użycia i modelach wdrożeniowych, ponieważ urządzenie zabezpieczające działa jako komponent PEP, a zarządzanie tymi urządzeniami działa jako komponent PE/PA. Podejście to wymaga, aby program zarządzania tożsamością (*ang. identity governance program – IGP*) w pełni funkcjonował, jednakże

opiera się na komponentach bramki, które działają jako PEP chroniący zasoby przed nieautoryzowanym dostępem lub ujawnieniem.

Kluczową koniecznością tego podejścia jest to, aby komponenty PEP były zarządzane i powinny być w stanie reagować i rekonfigurować się w razie potrzeby, aby reagować na zagrożenia lub zmiany w przepływie pracy. Możliwe jest zaimplementowanie w organizacji niektórych funkcji mikro-segmentacji przy użyciu mniej zaawansowanych urządzeń bramowych, a nawet bezstanowych firewalli, jednak koszty administracyjne i trudności w szybkim dostosowaniu się do zmian sprawiają, że jest to bardzo słaby wybór.

3.1.3. ZTA PRZY UŻYCIU INFRASTRUKTURY SIECIOWEJ I OBWODÓW ZDEFINIOWANYCH PROGRAMOWO

Ostatnie podejście do wdrożenia ZTA wykorzystuje infrastrukturę sieciową. Wdrożenie ZTA można osiągnąć poprzez wykorzystanie sieci nakładkowej (*ang. overlay network*), np. warstwy 7, ale można również wykorzystać niższą część stosu modelu sieci OSI. Podejścia te nazywane są czasami podejściami opartymi na obwodzie zdefiniowanym programowo (*ang. software defined perimeter – SDP*) i często obejmują koncepcje sieci zdefiniowanych programowo (*ang. Software Defined Networks – SDN*) [*SDNBOOK*] oraz sieci intuicyjnych (*ang. intent-based networking – IBNVN*) [*IBNVN*]. W podejściu tym PA działa jako sterownik sieci, który ustawia i rekonfiguruje sieć w oparciu o decyzje podjęte przez PE. Klienci nadal żądają dostępu za pośrednictwem PEP-ów, które są zarządzane przez komponent PA.

Gdy podejście to jest realizowane w sieciowej warstwie aplikacji (tzn. w warstwie 7), najczęstszym modelem wdrożenia jest agent/brama (patrz punkt 3.2.1). W tej implementacji bramka agenta i zasobu (działająca jako pojedynczy PEP i skonfigurowana przez PA) tworzy bezpieczny kanał służący do komunikacji pomiędzy klientem, a zasobem. Mogą istnieć inne warianty tego modelu, w tym również dla sieci wirtualnych w chmurze, sieci nie opartych na IP, itp.

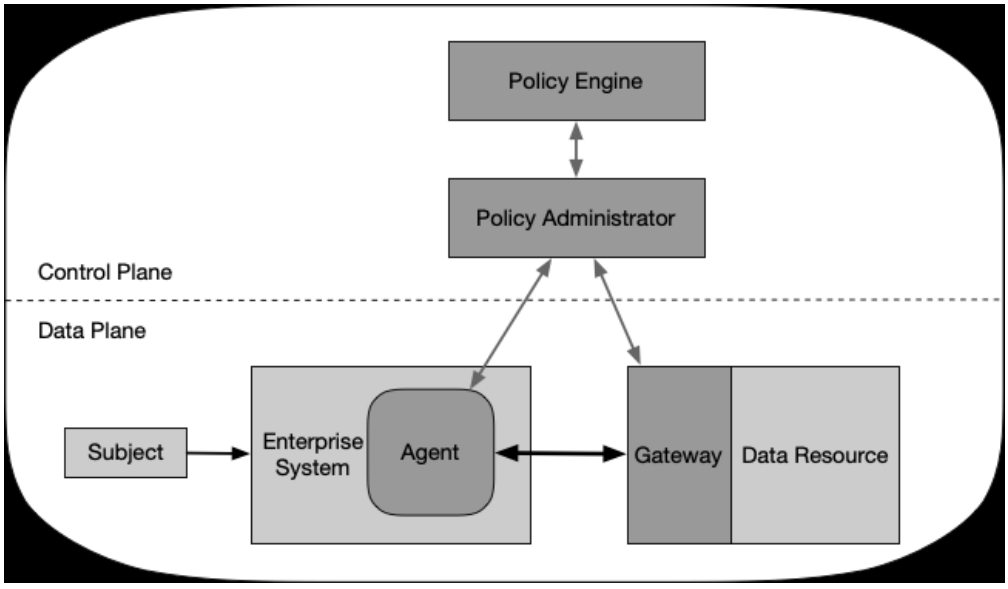
3.2. WDRAŻANIE WARIANTÓW ARCHITEKTURY ABSTRAKCYJNEJ

Wszystkie powyższe składniki są komponentami logicznymi. Nie muszą być one koniecznie unikatowymi systemami. Pojedynczy komponent aktywów do wykonywania zadań może wypełniać obowiązki wielu składników logicznych, podobnie składnik logiczny może składać się z wielu elementów sprzętowych lub programowych. Na przykład PKI zarządzana przez organizację może składać się z jednego składnika odpowiedzialnego za wydawanie certyfikatów dla urządzeń i drugiego używanego do wydawania certyfikatów użytkownikom końcowym, ale oba korzystają z pośrednich certyfikatów wydawanych przez ten sam główny organ certyfikacyjny organizacji. W niektórych dostępnych obecnie na rynku produktach ZT, komponenty PE i PA są połączone w jedną usługę.

Istnieje kilka wariantów rozmieszczenia wybranych komponentów architektury, które przedstawiono w poniższych sekcjach. W zależności od tego, jak zorganizowana jest sieć organizacji, do różnych procesów biznesowych w jednej organizacji może być stosowanych wiele modeli wdrożeniowych ZTA.

3.2.1. WDROŻENIE ROZWIĄZANIA BAZUJĄCEGO NA AGENTACH/BRAMACH PROGRAMOWYCH

W tym modelu wdrożenia, PEP jest podzielony na dwa komponenty, które znajdują się w zasobach lub jako komponent wdrożony bezpośrednio przed nimi. Na przykład, każde urządzenie udostępniane użytkownikowi przez organizację (np. laptop) posiada zainstalowanego agenta urządzenia, który koordynuje połączenia, a zasób (np. baza danych) posiada komponent (tj. bramę), który jest umieszczony bezpośrednio przed tym zasobem, tak że zasób komunikuje się tylko poprzez bramą, zasadniczo służąc jako proxy dla tego zasobu. Agent jest komponentem oprogramowania, który kieruje część (lub całość) ruchu do odpowiedniego PEP w celu oceny zgłoszeń. Bramka jest odpowiedzialna za komunikowanie się z administratorem zasad i zezwala tylko na zatwierdzone ścieżki komunikacji skonfigurowane przez administratora zasad (patrz Rysunek 3).



Rysunek 3. Model bazujący na agentach/bramach programowych[6]

W typowym scenariuszu podmiot (*ang. subject*) posiadający laptopa firmowego chce się podłączyć do zasobów (*ang. enterprise system*) organizacji (np. aplikacji/bazy danych zasobów ludzkich). Wniosek o dostęp jest pobierany przez lokalnego agenta (*ang. agent*), a następnie przekazywany do administratora zasad (*ang. policy administrator*). Administratorem zasad i mechanizmem (silnikiem) zasad (*ang. policy engine*) może być

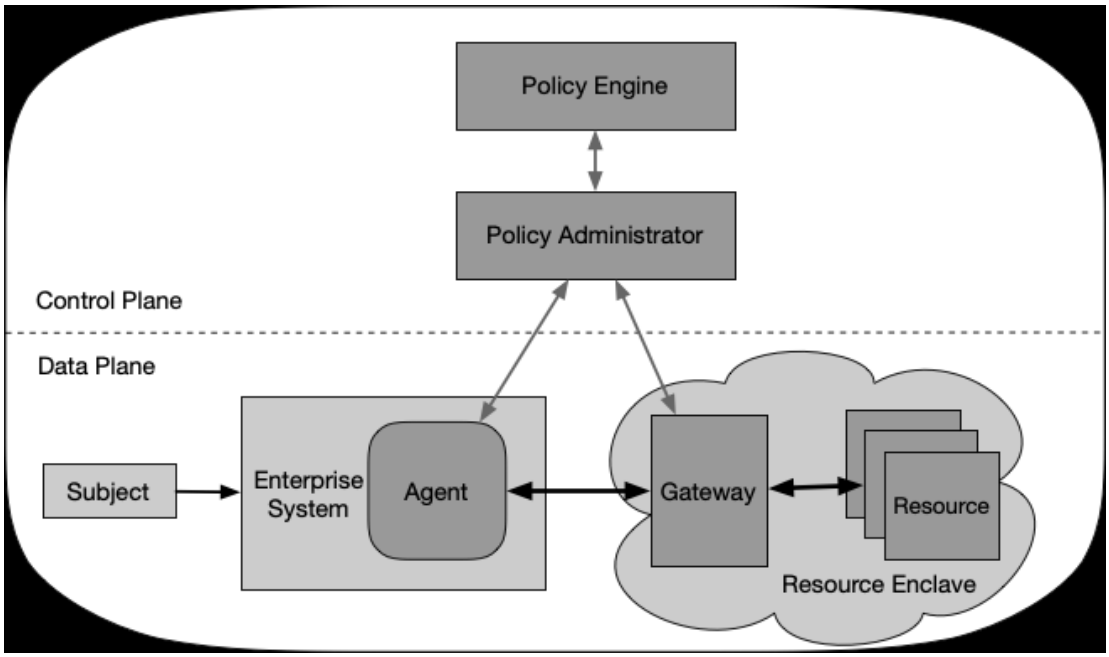
[6] Rozwinięcie angielskich nazw znajduje się w tekście w akapicie pod rysunkiem 3.

lokalny zasób organizacji lub usługa w chmurze. Administrator zasad przekazuje wniosek do mechanizmu zasad w celu jego oceny. Jeśli żądanie zostanie autoryzowane, administrator zasad konfiguruje kanał komunikacji pomiędzy agentem urządzenia, a odpowiednią bramą zasobu (*ang. gateway*) poprzez płaszczyznę kontrolną (*ang. control plane*). Może on zawierać takie informacje jak adres protokołu internetowego (IP), informacje o porcie, klucz sesji lub podobne artefakty bezpieczeństwa. Następnie agent i bramka zasobu łączą się i rozpoczynają szyfrowane przepływy danych aplikacji/usług. Połączenie pomiędzy agentem urządzenia, a bramą zasobów zostaje przerwane po zakończeniu przepływu pracy lub po wyzwoleniu przez administratora zasad takiego działania z powodu zdarzenia bezpieczeństwa (np. przerwanie sesji, brak ponownego uwierzytelnienia).

Model ten jest najlepiej wykorzystywany przez organizacje, które posiadają zaawansowane narzędzia do zarządzania urządzeniami, jak również zasoby, które mogą komunikować się poprzez bramę. Dla organizacji, które w dużym stopniu korzystają z usług w chmurze, jest to implementacja typu klient-serwer oprogramowania Cloud Security Alliance (CSA) Software Defined Perimeter (SDP) [CSA-SDP]. Model ten jest również odpowiedni dla organizacji, które nie chcą stosować polityki BYOD. Dostęp jest możliwy tylko za pośrednictwem agenta urządzenia, który może być umieszczony w sprzęcie będącym własnością organizacji.

3.2.2. WDRAŻANIE W ENKLAWIE (ANG. ENCLAVE-BASED)

Ten model wdrożenia jest odmianą wyżej opisanego modelu agent/brama. W modelu tym komponenty bramki nie znajdują się przed poszczególnymi zasobami, lecz na granicy enklawy zasobów (np. lokalnego centrum danych), jak pokazano na rysunku 4. Zazwyczaj zasoby te pełnią jedną funkcję biznesową lub mogą nie być w stanie komunikować się bezpośrednio z bramą (np. starszy system baz danych, który nie posiada interfejsu programowania aplikacji (AP), który może być używany do komunikacji z bramą). Ten model wdrożenia może być również przydatny dla organizacji, które korzystają z mikro usług opartych na chmurze dla pojedynczych procesów biznesowych (np. powiadamianie użytkowników, wyszukiwanie w bazie danych, wypłacanie wynagrodzeń). W tym modelu cała chmura prywatna znajduje się za bramą.



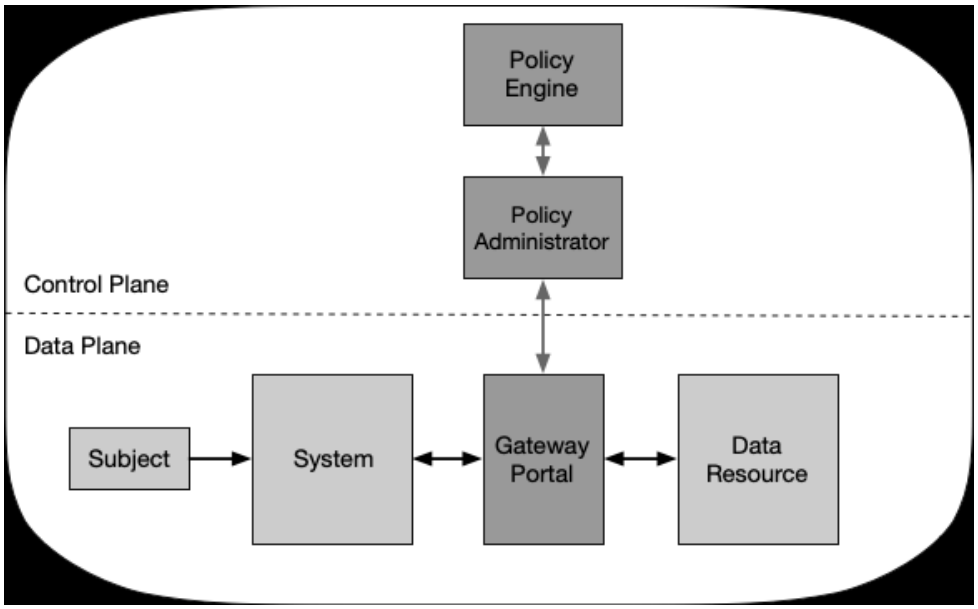
Rysunek 4. Model bramy enklawy

Możliwe jest hybrydowe połączenie tego modelu z modelem typu agent urządzenia /brama. W modelu tym zasoby organizacji mają agenta urządzenia, który jest używany do łączenia się z bramami enklawowymi, ale te połączenia są tworzone przy użyciu tego samego procesu co podstawowy model agent urządzenia/brama.

Model ten jest przydatny dla organizacji, które posiadają już istniejące aplikacje lub centra danych w lokalizacjach, które nie mogą posiadać indywidualnych bram. Organizacja potrzebuje zaawansowanego rozwiązania do zarządzania zasobami i konfiguracją, tak, aby zainstalować/konfigurować agentów urządzeń. Wadą jest to, że brama chroni zbiór zasobów i może nie być w stanie chronić każdego z nich z osobna. Może to również umożliwiać podmiotom dostęp do zasobów, do których nie mają uprawnień dostępu.

3.2.3. WDROŻENIE OPARTE O PORTALE ZASOBÓW (ANG. RESOURCE PORTAL-BASED)

W tym modelu wdrożenia, PEP jest pojedynczym komponentem, który działa jako bramka dla żądań tematycznych. Portal bramki może być przeznaczony dla pojedynczego zasobu lub bezpiecznej enklawy dla zbioru zasobów wykorzystywanych do jednej funkcji biznesowej. Jednym z przykładów może być portal bramki do chmury prywatnej lub centrum danych zawierającego starsze aplikacje, tak jak pokazano na rysunku 5.



Rysunek 5. Model portalu zasobów

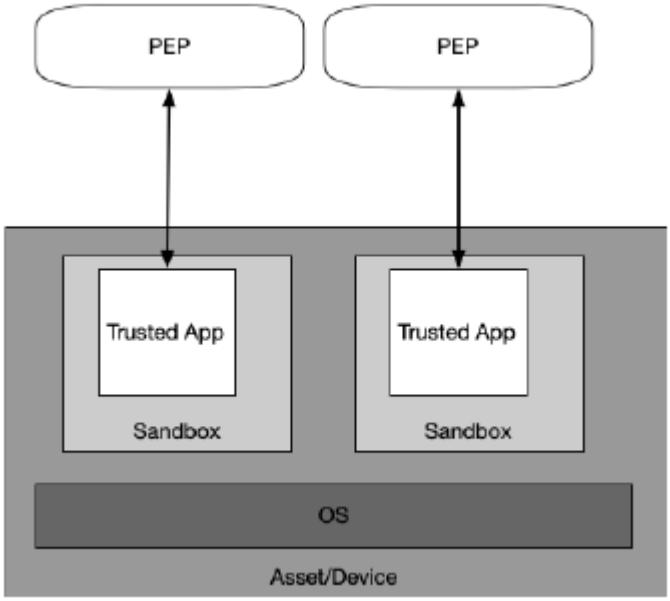
Podstawową zaletą tego modelu w porównaniu z innymi jest to, że komponent oprogramowania nie musi być instalowany na wszystkich urządzeniach klienckich. Model ten jest również bardziej elastyczny w przypadku polityki BYOD i projektów współpracy międzyorganizacyjnej. Administratorzy organizacji nie muszą upewniać się, że każde urządzenie posiada odpowiedniego agenta urządzenia. Mogą jednak uzyskać ograniczone informacje z urządzeń żądających dostępu. Model ten może skanować oraz analizować zasoby i urządzenia tylko po ich podłączeniu do portalu PEP i może nie być w stanie stale monitorować ich pod kątem złośliwego oprogramowania, nieusuniętych podatności i stosowania odpowiedniej konfiguracji.

Główną różnicą w tym modelu jest brak lokalnego agenta, który obsługuje żądania, a więc organizacja może nie mieć pełnej widoczności lub arbitralnej kontroli nad aktywami, ponieważ może je zobaczyć/skanować tylko wtedy, gdy połączą się one z portalem. W celu złagodzenia lub zrekompensowania takiego stanu rzeczy organizacja może zastosować takie środki, jak izolacja przeglądarki. Aktywa mogą być niewidoczne dla organizacji w okresie pomiędzy sesjami. Model ten pozwala również atakującym na ujawnienie i próbę uzyskania dostępu do portalu lub próbę ataku typu denial-of-service (DoS) na portal. Systemy portalowe powinny być dobrze wyposażone, aby zapewnić przeciwdziałanie atakowi DoS lub zakłóceniom sieci.

3.2.4. ŚRODOWISKO IZOLOWANE APLIKACJI NA URZĄDZENIU

Inną wariacją modelu wdrażania modelu agent/brama jest posiadanie sprawdzonych aplikacji lub procesów uruchamianych w oddzielnych zasobach. Zasoby te mogą być maszynami wirtualnymi, kontenerami lub inną implementacją, ale cel jest ten sam: ochrona

aplikacji lub instancji aplikacji przed potencjalnie zagrożonym hostem lub innymi aplikacjami działającymi na danym urządzeniu.



Rysunek 6. Środowisko izolowane (Sandboxing) aplikacji.[7]

Na rys. 6 urządzenie podmiotu (użytkownika) posiada zatwierdzoną, zaufaną aplikację (*ang. trusted app*) umieszczoną w środowisku izolowanym (*ang. sandbox*). Aplikacje muszą komunikować się z PEP, aby poprosić o dostęp do zasobów, ale PEP odrzuci wnioski z innych aplikacji na urządzeniu. W tym modelu PEP może być usługą lokalną organizacji lub usługą w chmurze.

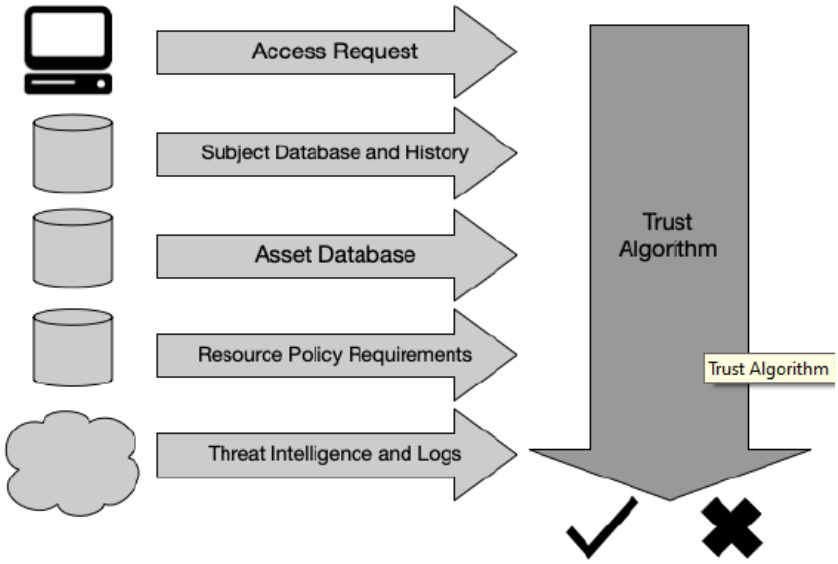
Główną zaletą tego wariantu jest to, że poszczególne aplikacje są oddzielone od reszty aktywów/urządzeń (*ang. asset/device*). Jeśli całe urządzenie nie może zostać przeskanowane w poszukiwaniu podatności, to przynajmniej aplikacje znajdujące się w środowisku izolowanym mogą być chronione przed potencjalną infekcją złośliwym oprogramowaniem. Jedną z wad tego modelu jest to, że organizacje muszą utrzymywać środowiska izolowane aplikacji dla wszystkich aktywów i mogą nie mieć pełnej widoczności aktywów klientów. Organizacja musi również upewnić się, że każda izolowananaplikacja (typu "sandboxed") jest bezpieczna, co może wymagać większego wysiłku niż zwykłe monitorowanie urządzeń.

3.3. ZAUFANY ALGORYTM

W przypadku organizacji, która wdrożyła ZTA, silnik zasad może być postrzegany jako mózg, a algorytm zaufania PE jako podstawowy proces myślowy. Zaufany algorytm (*ang. trusted*

[7] Rozwinięcie angielskich nazw znajduje się w tekście w akapicie pod rysunkiem 6.

algorithm - TA) jest procesem stosowanym przez silnik zasad w celu ostatecznego przyznania lub odmowy dostępu do zasobów. Silnik zasad pobiera dane z wielu źródeł (patrz Sekcja 3): baza danych zasad z obserwowalnymi informacjami na temat podmiotów, atrybutów podmiotów i ról, historycznych wzorców zachowania podmiotów, źródeł informacji o zagrożeniach i innych źródeł. Proces ten można pogrupować w szerokie kategorie i zwizualizować jak na rysunku 7.



Rysunek 7. Dane wejściowe do zaufanego algorytmu.[8]

Występujące na rysunku 7 dane wejściowe mogą być podzielone na kategorie w oparciu o to, czego dostarczają algorytmowi zaufania.

- **Wniosek o dostęp (*ang. Access request*):** Jest to rzeczywiste żądanie wystosowane przez podmiot. Zasób, o który się wnioskuje, to pierwotnie wykorzystywane informacje, jednak korzysta się również z informacji o wnioskodawcy. Mogą one obejmować wersję systemu operacyjnego, używane oprogramowanie (np. czy aplikacja, której dotyczy prośba, pojawia się na liście zatwierdzonych aplikacji?) oraz poziom poprawek. W zależności od tych czynników i statusu w zakresie bezpieczeństwa zasobów, dostęp do zasobów może zostać ograniczony lub odmówiony.
- **Podmiotowa baza danych (*ang. subject database*):** Zawiera informacje "kim jest" wnioskujący o dostęp do zasobów [NIST SP 800-63]. Jest to zbiór podmiotów (ludzi i procesów) organizacji lub współpracowników oraz zbiór przypisanych atrybutów/uprzywilejowań podmiotów. Te przedmioty i atrybuty stanowią podstawę zasad dostępu do zasobów [NIST SP 800-162] [NISTIR 7987]. Tożsamości użytkowników mogą zawierać połączenie tożsamości logicznej (np. ID konta)

[8] Rozwinięcie angielskich nazw znajduje się w tekście w akapicie pod rysunkiem 7.

i wyników kontroli uwierzytelniania przeprowadzanych przez PEP. Atrybuty tożsamości, które mogą być brane pod uwagę przy określaniu poziomu zaufania, obejmują czas i geolokalizację. Zbiór uprawnień nadawanych wielu podmiotom może być postrzegany jako rola, ale uprawnienia powinny być nadawane podmiotowi indywidualnie, a nie tylko dlatego, że mogą one pasować do konkretnej roli w organizacji. Zbiór ten powinien być zakodowany i przechowywany w systemie zarządzania ID i bazie danych zasad. W niektórych wariantach może to również obejmować dane o zaobserwowanym w przeszłości zachowaniu podmiotu (patrz punkt 3.3.1).

- **Baza danych aktywów (*ang. asset database*):** Jest to baza danych, która zawiera znany status każdego składnika aktywów (i ewentualnie znanego składnika aktywów niebędącego własnością tej organizacji/BYOD) będącego własnością organizacji (do pewnego stopnia zarówno fizycznego, jak i wirtualnego). Jest ona porównywana z obserwowalnym statusem składnika zasobów składającego wniosek, a służących do przetwarzania i może zawierać wersję systemu operacyjnego, obecne oprogramowanie oraz jego integralność, lokalizację (lokalizację sieci i geolokalizację) i poziom poprawek. W zależności od stanu tych zasobów porównywanych z tą bazą danych, dostęp do aktywów może zostać ograniczony lub odmówiony.
- **Wymagania dotyczące polityki dostępu do zasobów (*ang. resource policy requirements*):** Ten zestaw zasad uzupełnia bazę danych identyfikatorów i atrybutów użytkownika [NIST SP 800-63] oraz definiuje minimalne wymagania dotyczące dostępu do zasobu. Wymagania mogą obejmować poziomy zabezpieczeń autoryzacji, takie jak lokalizacja sieci MFA (np. odmowa dostępu z zagranicznych adresów IP), wrażliwość danych oraz żądania konfiguracji zasobów. Wymagania te powinny być opracowane zarówno przez administratora danych (tj. osoby odpowiedzialne za dane), jak i osoby odpowiedzialne za procesy biznesowe wykorzystujące dane (tj. osoby odpowiedzialne za misję).
- **Wywiad na temat zagrożeń (*ang. threat intelligance*):** Jest to kanał informacyjny lub źródło informacji o ogólnych zagrożeniach i aktywnym złośliwym oprogramowaniu działającym w Internecie. Mogą to być również konkretne informacje o komunikacji widzianej z urządzenia, które mogą być podejrzane (np. zapytania o ewentualne węzły kierowania i kontroli złośliwego oprogramowania). Kanały te mogą być usługami zewnętrznymi lub informacjami wewnętrznymi (np. z SOC), a także mogą zawierać sygnatury ataków i środki łagodzące. Jest to jedyny komponent, który najprawdopodobniej będzie pod kontrolą usługi, a nie organizacji.

Waga znaczenia dla każdego źródła danych może być wbudowaną cechą algorytmu lub może być konfigurowana przez organizację. Wartości wag mogą być stosowane w celu odzwierciedlenia znaczenia źródła danych dla organizacji.

Ostateczne ustalenie jest następnie przekazywane do PA w celu jego wykonania. Zadaniem PA jest skonfigurowanie niezbędnych PEP w celu umożliwienia autoryzowanej komunikacji. W zależności od sposobu wdrożenia ZTA, może to obejmować wysyłanie wyników uwierzytelniania i informacji o konfiguracji połączenia do bram i agentów lub portali zasobów. PEP mogą również wstrzymać lub przerwać sesję komunikacyjną w celu ponownego uwierzytelnienia i ponownej autoryzacji połączenia zgodnie z wymogami zasad. PA jest również odpowiedzialny za wydanie polecenia przerwania połączenia zgodnie z zasadami (np. po upływie czasu oczekiwania, po zakończeniu przepływu pracy, z powodu alarmu bezpieczeństwa).

3.3.1. WARIANTY ZAUFANYCH ALGORYTMÓW

Istnieją różne sposoby wdrożenia TA. Różne podmioty wdrażające mogą chcieć różnie mierzyć powyższe czynniki w zależności od ich postrzeganego znaczenia. Istnieją jeszcze dwie inne główne cechy, które mogą być wykorzystane do różnicowania TA. Pierwszą z nich jest sposób, w jaki czynniki te są oceniane, czy to jako decyzje binarne, czy też ważone części całego "wyniku" lub poziomu zaufania. Druga to sposób, w jaki żądania są oceniane w stosunku do innych żądań tego samego podmiotu, aplikacji/usługi lub urządzenia.

- **Kryteria - versus - wyniki:** Pomoc techniczna oparta na kryteriach zakłada zestaw kwalifikowanych atrybutów, które muszą być spełnione przed udzieleniem dostępu do danego zasobu lub dopuszczeniem działania (np. odczyt/zapis). Kryteria te są konfigurowane przez organizację i powinny być niezależnie konfigurowane dla każdego zasobu. Dostęp jest przyznany lub działanie zastosowane do zasobu tylko wtedy, gdy wszystkie kryteria są spełnione. TA opierający się na wynikach oblicza poziom ufności na podstawie wartości dla każdego źródła danych i wag skonfigurowanych przez organizację. Jeżeli wynik jest większy niż skonfigurowana wartość progowa dla danego zasobu, dostęp jest przyznawany lub wykonywana jest akcja. W przeciwnym razie żądanie jest odrzucane lub zmniejszane są uprawnienia dostępu (np. dla pliku udzielany jest dostęp do odczytu, ale nie do zapisu).
- **Pojedynczy - versus - kontekstowy:** TA pojedynczy traktuje każdy wniosek indywidualnie i nie bierze pod uwagę historii wniosków o dostęp podczas jego oceny. Może to pozwolić na szybszą ocenę, ale istnieje ryzyko, że atak może pozostać niewykryty, jeśli pozostanie on w obrębie dozwolonej roli uczestnika. TA kontekstowy podczas oceny wniosków o dostęp bierze pod uwagę historię wnioskodawcy. Oznacza to, że PA musi utrzymywać pewne informacje na temat wszystkich wnioskodawców

i aplikacji, co powoduje, że wykrycie napastnika, który użyje skompromitowanych danych uwierzytelniających w celu uzyskania dostępu do informacji w sposób nietypowy dla danego wnioskodawcy może być bardziej prawdopodobne. Oznacza to również, że PE musi być informowany o zachowaniu użytkowników przez PA (i PEP), z którymi podmioty kontaktują się podczas komunikacji. Analiza zachowania podmiotu może być wykorzystana do stworzenia modelu akceptowalnego użytkowania, a odchylenia od tego zachowania mogą spowodować dodatkowe kontrole uwierzytelniania lub odmowę dostępu do zasobów.

Te dwa czynniki nie zawsze są od siebie zależne. Możliwe jest posiadanie TA, który przypisuje poziom zaufania do każdego podmiotu i/lub urządzenia i nadal rozpatruje każdy wniosek o dostęp niezależnie (tzn. pojedynczo). Kontekstowy TA bazujący na wynikach zapewniłyby jednak możliwość oferowania bardziej dynamicznej i szczegółowej kontroli dostępu, ponieważ wynik zapewnia aktualny poziom zaufania do konta wnioskodawcy i szybciej dostosowuje się do zmieniających się czynników niż statyczne zasady modyfikowane przez administratorów.

Najlepiej byłoby, gdyby algorytm zaufania ZTA miał kontekstowy charakter, ale nie zawsze byłoby to możliwe przy dostępnych dla organizacji komponentach infrastruktury. Kontekstowy TA może łagodzić zagrożenia, gdy atakujący pozostaje blisko "normalnego" zestawu wniosków o dostęp do zagrożonego konta podmiotu lub atakuje z wykorzystaniem informacji poufnych. Podczas definiowania i wdrażania algorytmów zaufania ważne jest zachowanie równowagi między bezpieczeństwem, użytecznością i efektywnością kosztową. Ciągłe nakłanianie podmiotu do ponownej autoryzacji wobec zachowań zgodnych z historycznymi trendami i normami dotyczącymi jego funkcji i roli w organizacji może prowadzić do problemów z użytecznością. Na przykład, jeśli pracownik działu kadr ma zwykle dostęp do 20-30 rekordów pracowniczych w typowym dniu roboczym, kontekstowa pomoc techniczna może wysłać ostrzeżenie, jeśli żądanie dostępu nagle przekroczy 100 rekordów w ciągu dnia. Kontekstowy asystent może również wysłać ostrzeżenie, jeśli ktoś składa wnioski o dostęp po normalnych godzinach pracy, ponieważ może to być atakujący, który filtruje zapisy przy użyciu zagrożonego konta HR. Są to przykłady, w których kontekstowy TA może wykryć atak, podczas gdy pojedynczy TA może nie wykryć nowego zachowania. W innym przykładzie, księgowy, który zwykle uzyskuje dostęp do systemu finansowego w normalnych godzinach pracy, próbuje teraz uzyskać dostęp do systemu w środku nocy z nierozpoznawalnej lokalizacji. Kontekstowy TA może wywołać alarm i wymagać od podmiotu spełnienia bardziej rygorystycznego poziomu zaufania lub innych kryteriów określonych w publikacji specjalnej NIST SP 800-63A.

Opracowanie zestawu kryteriów lub wartości wagowych/progowych dla każdego zasobu wymaga planowania i testowania. Administratorzy organizacji mogą napotkać problemy

podczas wstępnej implementacji ZTA, gdy wnioski o dostęp, które powinny być zatwierdzone, są odrzucane z powodu błędnej konfiguracji. Skutkiem tego będzie wstępna faza "strojenia" wdrożenia. Konieczne może być dostosowanie kryteriów lub wag punktowych w celu zapewnienia, że zasady są egzekwowane, a jednocześnie pozwalają na funkcjonowanie procesów biznesowych przedsiębiorstwa. Czas trwania tej fazy strojenia zależy od zdefiniowanych przez organizację mierników służących przyznawaniu dostępu oraz tolerancji dla niepoprawnych odmów dostępu/zatwierdzeń dla zasobów wykorzystywanych w przepływie pracy.

3.4. KOMPONENTY SIECI / ŚRODOWISKA

W środowisku ZT powinno istnieć rozdzielenie (logiczne lub ewentualnie fizyczne) przepływów komunikacyjnych wykorzystywanych do sterowania i konfigurowania sieci oraz przepływów komunikacyjnych aplikacji / usług wykorzystywanych do wykonywania faktycznej pracy organizacji. Często dzieli się to na płaszczyznę sterowania siecią i płaszczyznę danych dla komunikacji aplikacji / usługi [Gilman].

Płaszczyzna sterowania jest używana przez różne komponenty infrastruktury (zarówno należące do organizacji, jak i od dostawców usług) do obsługi i konfigurowania zasobów, oceny, przyznawania lub odmawiania dostępu do zasobów i wykonania wszystkich niezbędnych operacji w celu ustanowienie ścieżki komunikacji między zasobami. Płaszczyzna danych służy do faktycznej komunikacji między komponentami oprogramowania. Ten kanał komunikacyjny może nie być zestawiony, zanim ścieżka ta nie zostanie ustanowiona przez płaszczyznę sterowania. Na przykład płaszczyzna sterowania może być używana przez PA i PEP do ustanowienia ścieżki komunikacyjnej między podmiotem, a zasobem organizacji. Obciążenie aplikacji/usługi będzie wtedy wykorzystywało ścieżkę płaszczyzny danych, która została ustalona.

3.4.1. WYMAGANIA DLA SIECI SŁUŻĄCE WSPARCIU ZTA

1. Aktywa organizacji mają podstawową łączność sieciową. Sieć lokalna (LAN), kontrolowana (lub nie kontrolowana) przez przedsiębiorstwo, zapewnia podstawowy routing i infrastrukturę (np. DNS). Zdalny składnik aktywów organizacji niekoniecznie musi korzystać ze wszystkich usług infrastrukturalnych.
2. Organizacja musi być w stanie odróżnić, jakie aktywa są jej własnością lub są przez nią zarządzane, od bieżącego statusu urządzeń w zakresie bezpieczeństwa. Określa się to na podstawie danych uwierzytelniających wydanych przez organizację, a nie na podstawie informacji, które nie mogą być uwierzytelnione (np. sieciowe adresy MAC, które mogą być sfałszowane).

3. Organizacja powinna obserwować cały ruch sieciowy. Organizacja rejestruje pakiety widziane na płaszczyźnie danych, nawet jeśli nie jest w stanie przeprowadzić inspekcji warstwy aplikacji (tj. warstwy 7 OSI) we wszystkich pakietach. Filtruje metadane dotyczące połączenia (np. miejsce docelowe, czas, tożsamość urządzenia), aby dynamicznie aktualizować zasady i informować jednostkę centralną podczas oceny żądań dostępu.
4. Zasoby organizacji nie powinny być dostępne bez dostępu do PEP. Zasoby organizacji nie przyjmują arbitralnych połączeń przychodzących z Internetu. Zasoby akceptują niestandardowo skonfigurowane połączenia dopiero po uwierzytelnieniu i autoryzacji klienta. Ścieżki komunikacyjne są konfigurowane przez PEP. Zasoby mogą nie być nawet wykrywalne bez dostępu do PEP. Uniemożliwia to napastnikom identyfikację celów poprzez skanowanie i/lub przeprowadzanie ataków DoS na zasoby znajdujące się za PEP. Należy pamiętać, że nie wszystkie zasoby powinny być ukryte w ten sposób; niektóre elementy infrastruktury sieciowej (np. serwery DNS) muszą być dostępne.
5. Płaszczyzna danych i płaszczyzna sterowania są logicznie oddzielone. Silnik zasad, administrator zasad i PEP komunikują się w sieci, która jest logicznie oddzielona i nie jest bezpośrednio dostępna dla zasobów i aktywów organizacji. Płaszczyzna danych jest wykorzystywana do przesyłania danych dotyczących aplikacji/usług. Silnik zasad, administrator zasad i PEP wykorzystują płaszczyznę sterowania do komunikacji i zarządzania ścieżkami komunikacyjnymi między aktywami. PEP muszą być w stanie wysyłać i odbierać komunikaty zarówno z płaszczyzny danych, jak i z płaszczyzny sterowania.
6. Aktywa organizacji muszą docierać do składnika PEP. Podmioty organizacji muszą mieć możliwość dostępu do komponentu PEP, aby uzyskać dostęp do zasobów. Może to przybrać formę portalu internetowego, urządzenia sieciowego lub agenta oprogramowania w urządzeniach organizacji, który umożliwi połączenie.
7. Komponent PEP jest jedynym komponentem, który uzyskuje dostęp do administratora zasad w ramach przepływu biznesowego. Każdy PEP działający w sieci organizacji ma połączenie z administratorem zasad w celu ustanowienia ścieżek komunikacji od klientów do zasobów. Cały ruch procesów biznesowych organizacji przechodzi przez jeden lub więcej PEP.
8. Zdalne aktywa organizacji powinny mieć możliwość dostępu do jej zasobów bez konieczności uprzedniego przemierzania infrastruktury sieci korporacyjnej. Na przykład, zdalny podmiot nie powinien być zobowiązany do korzystania z łącza z powrotem do sieci organizacji (tj. wirtualnej sieci prywatnej [VPN]) w celu uzyskania dostępu do usług wykorzystywanych przez przedsiębiorstwo i hostowanych przez dostawcę usług w chmurze publicznej (np. poczty elektronicznej).

9. Infrastruktura wykorzystywana do wspomagania procesu podejmowania decyzji o dostępie do ZTA powinna być skalowalna w celu uwzględnienia zmian w obciążeniu procesu. PE, PA i PEP wykorzystywane w ZTA stają się kluczowymi elementami każdego procesu biznesowego. Opóźnienie lub niezdolność do osiągnięcia PEP (lub niezdolność PEP do osiągnięcia PA/PE) ma negatywny wpływ na zdolność do wykonania przepływu pracy. Organizacja wdrażająca ZTA musi dostarczyć komponenty dla oczekiwanego obciążenia pracą lub być w stanie szybko skalować infrastrukturę, aby w razie potrzeby obsłużyć zwiększone wykorzystanie.
10. Aktywa organizacji mogą nie być w stanie dotrzeć do niektórych PEP z powodu zasad lub możliwych do zaobserwowania czynników. Na przykład, może istnieć zasada stanowiąca, że aktywa ruchome mogą nie być w stanie dotrzeć do pewnych zasobów, jeżeli aktywa, których dotyczy wniosek, znajdują się poza krajem pochodzenia organizacji. Czynniki te mogą wynikać z lokalizacji (geolokalizacja lub lokalizacja sieci), typu urządzenia lub innych kryteriów.

4. SCENARIUSZE WDRAŻANIA/PRZYPADKI UŻYCIA

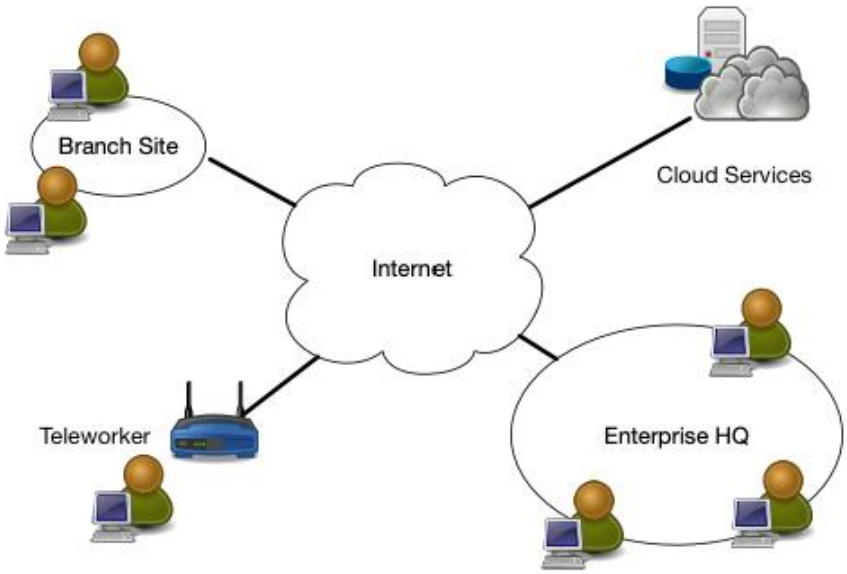
Każde środowisko korporacyjne powinno być zaprojektowane z myślą o zasadach braku zaufania. Większość organizacji ma już pewne elementy zerowego zaufania w swojej infrastrukturze korporacyjnej lub jest w trakcie wdrażania polityki bezpieczeństwa i odporności informacji oraz najlepszych praktyk. Kilka scenariuszy wdrożeniowych i przypadków użycia łatwo nadaje się do implementacji w ramach architektury "zero zaufania". Na przykład, ZTA ma swoje korzenie w organizacjach, które są rozproszone geograficznie i/lub posiadają wysoce mobilny personel. Niemniej jednak, każda organizacja może czerpać korzyści z architektury zerowego zaufania.

W poniższych przypadkach zastosowanie ZTA nie jest wyraźnie wskazane, ponieważ przedsiębiorstwo prawdopodobnie dysponuje zarówno infrastrukturą obwodową, jak i ewentualnie ZTA. Jak omówiono w sekcji 7.2, prawdopodobnie nastąpi okres, w którym komponenty ZTA i infrastruktura sieciowa oparta na obwodach będą jednocześnie eksploatowane w organizacjach.

4.1. ORGANIZACJE Z OBIEKTAMI ROZPROSZONYMI GEOGRAFICZNIE

Najczęstszy scenariusz dotyczy organizacji z jedną siedzibą główną i jedną lub więcej lokalizacjami rozproszonymi geograficznie, do których nie są dołączane fizyczne połączenia sieciowe należące do organizacji (zob. rys. 8). Aby wykonywać swoje zadania, pracownicy w odległych lokalizacjach mogą nie mieć pełnej sieci lokalnej należącej do organizacji, ale nadal muszą mieć dostęp do jej zasobów. Organizacja może posiadać łącze Multiprotocol Label Switch (MPLS) do sieci zlokalizowanej w kwaterze organizacji, ale może nie mieć odpowiedniej przepustowości dla całego ruchu lub może nie chcieć, aby ruch przeznaczony dla aplikacji/usług opartych na chmurze przechodził przez tą sieć. Podobnie, pracownicy mogą pracować zdalnie lub w oparciu o telepracę i korzystać z urządzeń będących własnością przedsiębiorstwa lub osób prywatnych. W takich przypadkach organizacja może chcieć przyznać dostęp do niektórych zasobów (np. kalendarza pracowników, poczty elektronicznej), ale odmówić dostępu lub ograniczyć działania do bardziej wrażliwych zasobów (np. bazy danych kadr).

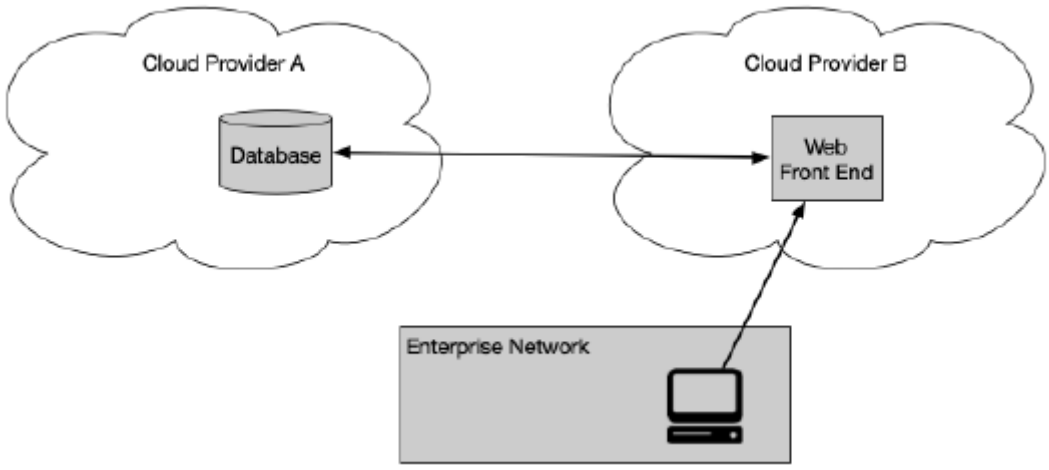
W tym przypadku zastosowania PE/PA są często hostowane jako usługa w chmurze (która zwykle zapewnia lepszą dostępność i nie wymaga od pracowników zdalnych polegania na infrastrukturze organizacji w celu uzyskania dostępu do zasobów w chmurze), przy czym aktywa końcowe mają zainstalowanego agenta (patrz punkt 3.2.1) lub dostęp do portalu zasobów (patrz punkt 3.2.3). Może nie być najodpowiedniejsze umieszczenie PE/PA w lokalnej sieci organizacji, ponieważ zdalne biura i pracownicy muszą odesłać cały ruch z powrotem do sieci organizacji, aby korzystać z aplikacji/usług hostowanych przez usługi w chmurze.



Rysunek 8. Organizacja ze zdalnymi pracownikami.

4.2. ORGANIZACJA DZIAŁAJĄCA W MODELU WIELOCHMUROWYM

Jednym z coraz częstszych przypadków zastosowania ZTA są organizacje wykorzystujące wielu dostawców usług w chmurze (patrz Rysunek 9). W tym przypadku zastosowania, organizacja posiada sieć lokalną, ale korzysta z dwóch lub więcej dostawców usług w chmurze do hostowania aplikacji/usług i danych. Czasami aplikacja/usługa jest hostowana w usłudze w chmurze, która jest oddzielona od źródła danych. W celu zapewnienia wydajności i łatwości zarządzania, aplikacja hostowana u dostawcy usługi w chmurze A powinna być w stanie połączyć się bezpośrednio ze źródłem danych hostowanym u dostawcy usługi w chmurze B, a nie zmuszać aplikację do tunelowania z powrotem przez sieć organizacji.

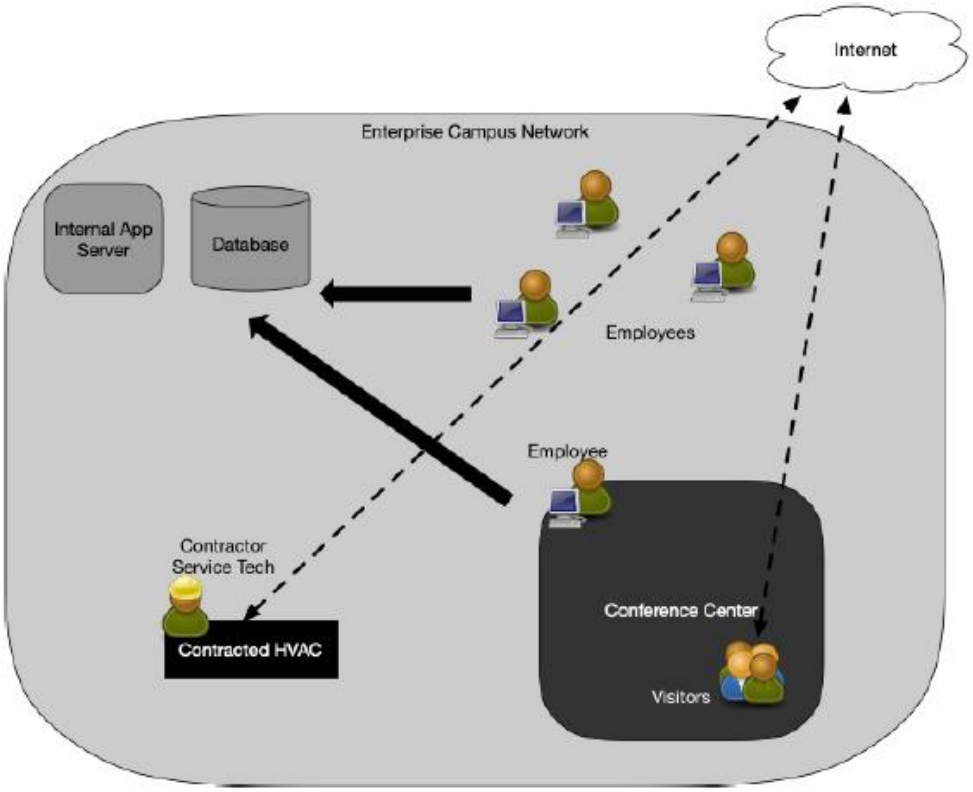


Rysunek 9. Przypadek użycia modelu wielochmurowego

Ten przypadek użycia jest implementacją typu serwer - serwer CSA obwodu definiowanego programowo (SDP) [CSA-SDP]. W miarę jak organizacje stosują większe ilości aplikacji i usług w chmurze, staje się oczywiste, że poleganie na ochronie obwodowej staje się wyzwaniem. Jak omówiono w sekcji 2.2, zasady ZT wyrażają pogląd, że nie powinno być różnicy między infrastrukturą sieciową będącą własnością organizacji i infrastrukturą obsługiwaną przez organizację, a infrastrukturą będącą własnością i obsługiwaną przez jakiegokolwiek innego dostawcę usług. Podejście oparte na zasadzie "zero zaufania" do korzystania z wielu chmur polega na umieszczaniu PEP w punktach dostępu w każdej aplikacji/usłudze i źródle danych. PEP i PA mogą być usługami zlokalizowanymi w chmurze lub nawet u trzeciego dostawcy usług w chmurze. Następnie klient (za pośrednictwem portalu lub lokalnie zainstalowanego agenta) uzyskuje bezpośredni dostęp do PEP. W ten sposób organizacja może nadal zarządzać dostępem do zasobów nawet wtedy, gdy są one hostowane poza organizacją. Jednym z wyzwań jest to, że różni dostawcy usług w chmurze mają unikatowe sposoby wdrażania podobnych funkcjonalności. Architekci korporacyjni będą musieli być świadomi, w jaki sposób wdrożyć ZTA swojej organizacji u każdego dostawcy chmury, z którego usług korzystają.

4.3. ORGANIZACJA Z USŁUGAMI KONTRAKTOWYMI I/LUB DOSTĘPEM DLA OSÓB NIEBĘDĄCYCH PRACOWNIKAMI

Innym powszechnym scenariuszem jest taki, który obejmuje osoby nie będące pracownikami, działające w siedzibie organizacji i/lub zakontraktowanych usługodawców, którzy wymagają ograniczonego dostępu do zasobów organizacji w celu wykonywania swojej pracy (zob. rys. 10). Na przykład, organizacja posiada własne wewnętrzne aplikacje/usługi, bazy danych i aktywa. Obejmują one usługi zlecane usługodawcom, którzy mogą okazjonalnie przebywać w siedzibie organizacji w celu zapewnienia obsługi (np. inteligentne systemy grzewcze i oświetleniowe, które są własnością i są zarządzane przez dostawców zewnętrznych). Ci goście i dostawcy usług będą potrzebowali łączności sieciowej, aby wykonywać swoje zadania. Organizacja posiadająca wdrożoną ZTA mogłoby to ułatwić, umożliwiając tym urządzeniom i każdemu odwiedzającemu serwisantowi dostęp do Internetu przy jednoczesnym zasłanianiu zasobów organizacji.



Rysunek 10. Organizacja z dostępem dla osób nie będących pracownikami.

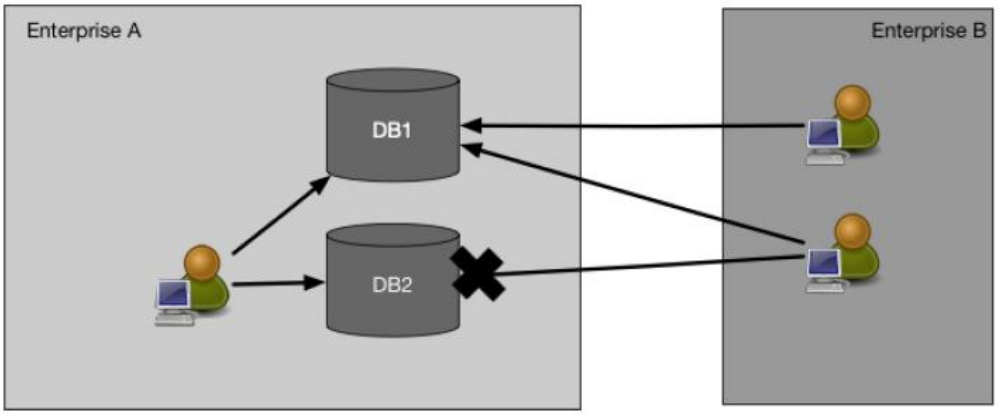
W tym przykładzie organizacja posiada również centrum konferencyjne, w którym odwiedzający wchodzą w interakcję z pracownikami. Również w tym przypadku, dzięki podejściu ZTA SDP, urządzenia i podmioty są zróżnicowane i mogą mieć dostęp do odpowiednich zasobów organizacji. Odwiedzający siedzibę mogą mieć dostęp do Internetu, ale nie mogą mieć dostępu do zasobów organizacji. Mogą nawet nie być w stanie odkryć usług przedsiębiorstwa za pomocą skanów sieciowych (tj. nie ma możliwości aktywnego rozpoznanie sieci).

W tym przypadku, PE i PA mogą być hostowane jako usługa w chmurze lub w sieci LAN (zakładając niewielkie wykorzystanie usług w chmurze lub brak takiego wykorzystania). Aktywa organizacji mogą mieć zainstalowanego agenta (zob. pkt 3.2.1) lub dostęp do zasobów za pośrednictwem portalu (zob. pkt 3.2.3). PA gwarantuje, że wszystkie urządzenia niebędące własnością organizacji (tj. te, które nie mają zainstalowanych agentów lub nie mogą połączyć się z portalem) nie mają dostępu do zasobów lokalnych, ale mogą mieć dostęp do Internetu.

4.4. WSPÓŁPRACA POPRZEZ GRANICE ORGANIZACJI

Czwarty przypadek użycia to współpraca między organizacjami. Na przykład, istnieje projekt angażujący pracowników z przedsiębiorstw A i B (patrz Rysunek 11). Te dwie organizacje

mogą być odrębnymi urzędami państwowymi (G2G) lub urzędem państwowym i przedsiębiorstwem prywatnym (G2B). Organizacja A obsługuje bazę danych wykorzystywaną w projekcie, ale musi umożliwić dostęp do danych niektórym członkom Organizacji B. Organizacja A może założyć specjalistyczne konta dla pracowników Organizacji B, aby mogła ona uzyskać dostęp do wymaganych danych i odmówić dostępu do wszystkich innych zasobów, ale może to szybko stać się trudne do zarządzania. Wpisanie obu organizacji do jednego z systemów zarządzania ID pozwoliłoby na szybsze nawiązanie tych relacji, pod warunkiem, że PEP obu organizacji będą w stanie uwierzytelnić podmioty w zjednoczonej społeczności ID.



Rysunek 11. Współpraca pomiędzy organizacjami.

Ten scenariusz może być podobny do przypadku użycia przypadku 1 (punkt 4.1), ponieważ pracownicy obu organizacji mogą nie znajdować się w infrastrukturze sieciowej ich organizacji, a zasoby, do których muszą mieć dostęp, mogą znajdować się w jednym środowisku organizacji lub być umieszczone w chmurze. Oznacza to, że nie muszą istnieć złożone reguły zapory sieciowej lub listy kontroli dostępu (ACL) w całej organizacji umożliwiające niektórym adresom IP należącym do organizacji B dostęp do zasobów w organizacji A w oparciu o zasady dostępu organizacji A. Sposób uzyskania tego dostępu zależy od stosowanej technologii. Podobnie jak w przypadku 1, PE i PA hostowane jako usługa w chmurze mogą zapewnić dostępność dla wszystkich stron, bez konieczności tworzenia VPN lub podobnych kanałów komunikacji. Pracownicy organizacji B mogą zostać poproszeni o zainstalowanie agenta oprogramowania na swoim sprzęcie lub uzyskanie dostępu do niezbędnych zasobów danych za pośrednictwem bramki internetowej (patrz Punkt 3.2.3).

4.5. ORGANIZACJE ŚWIADCZĄCE USŁUGI DLA ZAREJESTROWANYCH UŻYTKOWNIKÓW PUBLICZNYCH

Wspólną cechą w wielu organizacji jest usługa publiczna, która może, ale nie musi zawierać rejestrację użytkownika (tzn. użytkownicy muszą utworzyć lub otrzymać zestaw danych uwierzytelniających do logowania). Usługi takie mogą być przeznaczone dla ogółu społeczeństwa, dla grupy klientów mających istniejące relacje biznesowe lub dla specjalnej grupy użytkowników spoza organizacji, takich jak osoby pozostające na utrzymaniu pracownika. We wszystkich przypadkach jest prawdopodobne, że używane urządzenia nie jest własnością organizacji oraz, że organizacja nie ma pojęcia o stosowanych u takich użytkowników zasadach cyberbezpieczeństwa.

W przypadku ogólnych, publicznie dostępnych zasobów, do których dostęp nie wymaga podania danych do logowania (np. publicznej strony internetowej), zasady ZTA nie mają bezpośredniego zastosowania. Organizacja nie może ściśle kontrolować stanu urządzeń, a anonimowe zasoby publiczne (np. publiczna strona internetowa) nie wymagają uwierzytelnienia w celu uzyskania dostępu.

Organizacja może ustanowić zasady dla zarejestrowanych użytkowników publicznych, takich jak klienci (np. ci, z którymi utrzymuje relacje biznesowe) oraz użytkownicy specjalni (np. osoby pozostające na utrzymaniu pracowników). Jeżeli od użytkowników wymaga się przedstawienia lub wydaje się dane uwierzytelniające, organizacja może ustanowić zasady dotyczące długości hasła, cyklu życia i innych szczegółów oraz może dostarczyć MFA jako opcję lub wymóg. Jednakże organizacje mają ograniczoną liczbę zasad, które mogą wdrożyć dla tej klasy użytkowników. Informacje o przychodzących żądaniach mogą być użyteczne przy określaniu stanu usługi publicznej i wykrywaniu możliwych ataków maskujących się jako prawowici użytkownicy. Wiadomo na przykład, że zarejestrowani klienci mają dostęp do zarejestrowanego portalu użytkownika za pomocą jednej z wielu popularnych przeglądarek internetowych. Nagły wzrost liczby żądań dostępu z nieznanych typów przeglądarek lub znanych nieaktualnych wersji może wskazywać na pewien rodzaj automatycznego ataku, a organizacja może podjąć kroki w celu ograniczenia liczby żądań od tych klientów. Organizacja powinna również znać wszelkie statuty i regulacje dotyczące tego, jakie informacje o żądających użytkownikach i aktywach mogą być gromadzone i rejestrowane.

5. ZAGROŻENIA ZWIĄZANE Z ARCHITEKTURĄ „ZERO ZAUFANIA”

Żadna organizacja nie jest w stanie wyeliminować ryzyka związanego z cyberbezpieczeństwem. Prawidłowo wdrożony i utrzymywany system ZTA, po uzupełnieniu go o istniejące zasady i wytyczne dotyczące cyberbezpieczeństwa, zarządzania tożsamością i dostępem, stałego monitorowania i ogólnej cyberhigieny, może zmniejszyć ogólne ryzyko i chronić się przed powszechnymi zagrożeniami. Niektóre zagrożenia mają jednak wyjątkowe cechy podczas wdrażania ZTA.

5.1. NARUSZENIE PROCESU DECYZYJNEGO ZTA

W ZTA silnik zasad i administrator zasad są kluczowymi elementami składowymi całego przedsięwzięcia. Komunikacja pomiędzy zasobami organizacji nie może mieć miejsca, jeśli nie zostanie zatwierdzona i ewentualnie skonfigurowana przez PE i PA. Oznacza to, że komponenty te muszą być odpowiednio skonfigurowane i utrzymywane. Każdy administrator organizacji mający dostęp do konfiguracji zasad programu PE może być w stanie dokonać niezatwierdzonych zmian lub popełnić błędy, które mogą zakłócić pracę organizacji. Podobnie skompromitowany moduł PA może umożliwiać dostęp do zasobów, który w przeciwnym razie nie zostałyby zatwierdzony (np. do skompromitowanego urządzenia, będącego własnością prywatną). Łagodzenie związanych z tym zagrożeń oznacza, że komponenty PE i PA muszą być odpowiednio skonfigurowane i monitorowane, a wszelkie zmiany konfiguracji muszą być rejestrowane i poddawane audytowi.

5.2. ATAK DENIAL-OF-SERVICE LUB DEGRADACJA SIECI

W ZTA, PA jest kluczowym komponentem dla dostępu do zasobów. Zasoby organizacji nie mogą łączyć się ze sobą bez zgody PA i ewentualnie akcji konfiguracyjnej. Jeśli atakujący zakłóca lub odmawia dostępu do PEP lub PE/PA (np. atak DoS lub atak na DNS), może to niekorzystnie wpłynąć na działalność organizacji. Organizacje mogą złagodzić to zagrożenie, umieszczając egzekwowanie zasad w odpowiednio zabezpieczonym środowisku chmury lub powielając je w kilku lokalizacjach zgodnie z wytycznymi dotyczącymi odporności w cyberprzestrzeni [NIST SP 800-160 v2].

Ogranicza to ryzyko, ale nie eliminuje go. Botnety takie jak Mirai powodują masowe ataki DoS przeciwko kluczowym dostawcom usług internetowych i zakłócają świadczenie usług milionom użytkowników Internetu. Możliwe jest również, że atakujący może przechwycić i zablokować ruch do PEP lub PA z części lub wszystkich kont użytkowników w organizacji (np. z oddziału lub nawet od jednego zdalnego pracownika). W takich przypadkach dotyczy to tylko części podmiotów w organizacji. Jest to również możliwe w przypadku dostępu poprzez VPN i nie jest to jedyne cecha ZTA.

Dostawca usług hostingowych może również przypadkowo odebrać w chmurze dostęp do PE lub PA. W usługach w chmurze w przeszłości występowały zakłócenia, zarówno w infrastrukturze jako usłudze IaaS, jak i w SaaS. Błąd operacyjny może uniemożliwić funkcjonowanie całej organizacji, jeżeli silnik zasad lub komponent administratora zasad stanie się niedostępny z sieci.

Istnieje również ryzyko, że zasoby organizacji mogą być nieosiągalne z PA, więc nawet jeśli dostęp do danego podmiotu zostanie przyznany, PA nie może skonfigurować ścieżki komunikacyjnej w sieci. Może to być spowodowane atakiem DDoS lub po prostu nieoczekiwanym intensywnym użytkowaniem. Jest to podobne do wszelkich innych zakłóceń w sieci, w wyniku których niektóre lub wszystkie podmioty w organizacji nie mogą uzyskać dostępu do danego zasobu, ponieważ z jakiegoś powodu jest on niedostępny.

5.3. KRADZIEŻ DANYCH UWIERZYTELNIAJĄCYCH/ZAGROŻENIE WEWNĘTRZNE

Prawidłowo wdrożone zasady ZT, bezpieczeństwa i odporności informacji oraz najlepsze praktyki zmniejszają ryzyko uzyskania przez napastnika szerokiego dostępu z wykorzystaniem skradzionych danych uwierzytelniających lub atak wewnętrzny. Zasada ZT polegająca na braku ukrytego zaufania w oparciu o lokalizację w sieci oznacza, że napastnik musi zagrozić istniejącym kontom lub urządzeniom w celu zdobycia pozycji do ataku w organizacji. Prawidłowo opracowana i wdrożona ZTA powinna uniemożliwiać skompromitowanemu kontu lub aktywowi uzyskanie dostępu do zasobów poza jego normalnym zasięgiem lub wzorcami dostępu. Oznacza to, że konta z zasadą dostępu do zasobów, którymi atakujący jest zainteresowany, byłyby dla niego głównym celem.

Atakujący mogą wykorzystywać phishing, inżynierię społeczną lub kombinację ataków w celu uzyskania danych uwierzytelniających cennych kont. „Cenne" może oznaczać różne rzeczy w oparciu o motywację atakującego. Na przykład, konta administratorów organizacji mogą być wartościowe, ale atakujący zainteresowani zyskami finansowymi mogą uznać za cenne konta, które mają dostęp do zasobów finansowych lub płatniczych. Wdrożenie MFA dla wniosków o dostęp może zmniejszyć ryzyko utraty informacji z zagrożonego konta. Jednak atakujący posiadający ważne dane uwierzytelniające (lub atakujący z wewnątrz) może nadal mieć dostęp do zasobów powiązanych z danym kontem. Na przykład atakujący lub złośliwy pracownik, który posiada poświadczenia i sprzęt organizacji należące do istotnego pracownika działu kadr, może nadal mieć dostęp do bazy danych pracowników.

ZTA zmniejsza ryzyko i zapobiega ruchom bocznym w sieci w stosunku do skompromitowanych kont lub aktywów. Jeśli skompromitowane dane uwierzytelniające nie są upoważnione do dostępu do konkretnego zasobu, nadal będzie się im odmawiało dostępu do tego zasobu. Ponadto istnieje większe prawdopodobieństwo, że kontekstowy algorytm

zaufania (zob. sekcja 3.3.1) wykryje ten atak i szybciej na niego zareaguje, niż w przypadku ataku w dotychczasowej sieci opartej na ochronie obwodu. Kontekstowy algorytm zaufania może wykryć wzorce dostępu, które nie są zgodne z normalnym zachowaniem i odmówić skompromitowanemu kontu lub osobie atakującej z wewnątrz dostępu do wrażliwych zasobów.

5.4. WIDOCZNOŚĆ W SIECI

Jak wspomniano w sekcji 3.4.1, cały ruch jest kontrolowany i rejestrowany w sieci oraz analizowany w celu identyfikacji i reagowania na potencjalne ataki na organizację. Jednakże, jak również wspomniano, część (prawdopodobnie większość) ruchu w sieci organizacji może być nieprzejrzysta dla narzędzi analizy sieci warstwy 3. Ruch ten może pochodzić z aktywów niebędących własnością organizacji (np. zakontraktowanych usług, które wykorzystują infrastrukturę organizacji do uzyskania dostępu do Internetu) lub aplikacji/usług, które są odporne na bierny monitoring. Organizacja, która nie może przeprowadzić dogłębnej kontroli pakietów lub zbadać zaszyfrowanego ruchu musi zastosować inne metody w celu rozpoznania ewentualnego napastnika w sieci.

Nie oznacza to, że organizacja nie jest w stanie analizować zaszyfrowanego ruchu, który widzi w sieci. Organizacja może zbierać metadane (np. adresy źródłowe i docelowe itp.) dotyczące zaszyfrowanego ruchu i wykorzystywać je do wykrywania aktywnego napastnika lub możliwego złośliwego oprogramowania komunikującego się w sieci. Do analizy ruchu, który nie może być odszyfrowany i zbadany mogą być wykorzystywane techniki uczenia maszynowego [Anderson]. Zastosowanie tego typu technik pozwoliłoby organizacji sklasyfikować ruch jako właściwy lub potencjalnie złośliwy i podlegający interwencji.

5.5. PAMIĘĆ MASOWA SYSTEMU I INFORMACJE SIECIOWE

Zagrożeniem związanym z monitorowaniem i analizą ruchu sieciowego w organizacji jest sam składnik analizy. Jeśli skany monitorujące, ruch sieciowy i metadane są przechowywane w celu tworzenia polityki kontekstowej, analizy kryminalistycznej lub późniejszych analiz, dane te stają się celem ataku. Podobnie jak topologia sieci, pliki konfiguracyjne i inne dokumenty dotyczące architektury sieciowej, zasoby te powinny być chronione. Jeśli atakujący może z powodzeniem uzyskać dostęp do tych informacji, może być w stanie uzyskać wgląd w architekturę korporacyjną i zidentyfikować zasoby do dalszego rozpoznania i ataku.

Innym źródłem informacji zwiadowczych dla atakującego w organizacji stosującej ZT jest narzędzie zarządzania wykorzystywane do kodowania polityk dostępu. Podobnie jak zapisywany ruch, komponent ten zawiera zasady dostępu do zasobów i może dostarczyć

napastnikowi informacji o tym, które konta są najcenniejsze jako cel ataku (np. te, które mają dostęp do pożądanych zasobów danych).

Jeśli chodzi o wszystkie cenne dane organizacji, należy wprowadzić odpowiednie zabezpieczenia, aby zapobiec nieautoryzowanemu dostępowi i próbom uzyskania dostępu do nich. Ponieważ zasoby te mają zasadnicze znaczenie dla bezpieczeństwa, powinny one posiadać najbardziej restrykcyjne zasady dostępu i być dostępne tylko z wyznaczonych lub dedykowanych kont administratorów.

5.6. STOSOWANIE AUTORSKICH FORMATÓW DANYCH LUB ROZWIĄZAŃ

Przy podejmowaniu decyzji o dostępie ZTA opiera się na kilku różnych źródłach danych, w tym na informacjach dotyczących podmiotu składającego wniosek, wykorzystywanego sprzętu, danych wywiadowczych oraz analizie zagrożeń. Często zdarza się, że aktywa wykorzystywane do przechowywania i przetwarzania tych informacji nie mają ogólnego, otwartego standardu dotyczącego sposobu interakcji i wymiany informacji. Może to prowadzić do przypadków, w których organizacja jest zamknięta w podzbiorze dostawców ze względu na kwestie związane z interoperacyjnością. Jeżeli u jednego z dostawców wystąpi problem lub zakłócenie bezpieczeństwa, organizacja może nie być w stanie przenieść się do nowego dostawcy bez poniesienia skrajnych kosztów (np. zastąpienia kilku aktywów) lub przejścia przez długi okres przejściowy (np. przetłumaczenia zasad z jednego zastrzeżonego formatu na inny). Podobnie jak w przypadku ataków DoS, ryzyko to nie jest unikatowe dla ZTA, ale ponieważ ZTA jest w dużym stopniu uzależniona od dynamicznego dostępu do informacji (zarówno organizacji, jak i dostawców usług), zakłócenie może mieć wpływ na podstawowe funkcje biznesowe. Aby ograniczyć związane z tym ryzyko, organizacje powinny oceniać dostawców usług w sposób całościowy, uwzględniając oprócz bardziej typowych czynników, takich jak kontrola bezpieczeństwa dostawców, koszty zmiany dostawcy oraz zarządzanie ryzykiem związanym z łańcuchem dostaw, takie jak wydajność, stabilność itp.

5.7. KORZYSTANIE Z USŁUG PODMIOTÓW NIEOSOBOWYCH[9] W ADMINISTRACJI ZTA

Do zarządzania bezpieczeństwem w sieciach organizacji wdrażane są sztuczne inteligencje i inne środki oparte na oprogramowaniu. Komponenty te muszą współdziałać z komponentami zarządzającymi ZTA (np. silnikiem zasad, administratorem zasad), czasami zamiast ludzkiego administratora. Sposób, w jaki komponenty te uwierzytelniają się w organizacji wdrażającej ZTA, jest kwestią otwartą. Zakłada się, że większość

[9] *ang. Non-person Entities – NPE.*

zautomatyzowanych systemów technologicznych użyje pewnych środków do uwierzytelniania przy użyciu API do komponentów zasobów.

Największym zagrożeniem przy stosowaniu zautomatyzowanej technologii do konfiguracji i egzekwowania zasad jest możliwość wystąpienia fałszywych wyników pozytywnych - poprawne działania uznane za atak (*ang. false positives*) i fałszywych wyników negatywnych - ataki uznane za poprawne działanie (ang. *false negatives*) mających wpływ na stan bezpieczeństwa organizacji. Można to ograniczyć dzięki analizie retrospektywnej w celu skorygowania błędnych decyzji i poprawy procesu decyzyjnego.

Związane z tym ryzyko polega na tym, że napastnik będzie w stanie nakłonić lub zmusić NPE do zezwolenia na wykonania jakiegoś zadania, do którego napastnik nie jest uprawniony. Agent oprogramowania może mieć niższy poziom uwierzytelniania (np. klucz API zamiast MFA) do wykonywania zadań administracyjnych lub związanych z bezpieczeństwem w porównaniu z ludzkim użytkownikiem. Jeśli napastnik może wchodzić w interakcję z agentem, teoretycznie może oszukać agenta, aby umożliwić mu większy dostęp lub wykonać jakieś zadanie w jego imieniu. Istnieje również ryzyko, że atakujący może uzyskać dostęp do danych agenta oprogramowania i podszywać się pod niego podczas wykonywania zadań.

6. ARCHITEKTURA ZERO TRUST I MOŻLIWE INTERAKCJE Z ISTNIEJĄCYMI WYTYCZNYMI

<nieadekwatne do warunków polskich>

7. MIGRACJA DO ARCHITEKTURY „ZERO ZAUFANIA”

Wdrożenie ZTA to raczej migracja niż hurtowa wymiana infrastruktury lub procesów. Organizacja powinna dążyć do stopniowego wdrażania zasad zerowego zaufania, zmian w procesach i rozwiązań technologicznych, które chronią jej zasoby danych o najwyższej wartości. Większość organizacji będzie nadal działać w trybie hybrydowym „zero zaufania”/ochrona granic systemu w czasie nieokreślonym, kontynuując jednocześnie inwestycje w bieżące inicjatywy w zakresie modernizacji IT. Posiadanie planu modernizacji IT, który obejmuje przejście na architekturę opartą na zasadach ZT, może pomóc organizacji w tworzeniu harmonogramów dla migracji na małą skalę.

To, w jaki sposób organizacja przejdzie na daną strategię, zależy od jego obecnego statusu i działań w zakresie cyberbezpieczeństwa. Organizacja powinna osiągnąć pewien poziom kompetencji, zanim możliwe stanie się wdrożenie znaczącego środowiska zorientowanego na ZT [ACT-IAC]. Ten poziom bazowy obejmuje zidentyfikowanie i skatalogowanie aktywów, podmiotów, procesów biznesowych, przepływów ruchu sieciowego i map zależności. Organizacja potrzebuje tych informacji, zanim będzie mogła opracować listę kandydujących procesów biznesowych oraz podmiotów/aktywów zaangażowanych w ten proces.

7.1. PRZEJRZYSTA ARCHITEKTURA „ZERO ZAUFANIA”

W podejściu typu ''niezabudowany teren” możliwe byłoby zbudowanie architektury „zero zaufania” od podstaw. Zakładając, że organizacja zna aplikacje/usługi i przepływy pracy, które chce wykorzystać w swoich działaniach, może ona stworzyć architekturę opartą na zasadach zerowego zaufania dla tych przepływów pracy. Po zidentyfikowaniu przepływów pracy, organizacja może zawęzić zakres potrzebnych komponentów i rozpocząć mapowanie interakcji pomiędzy poszczególnymi komponentami. Od tego momentu jest to działanie inżynieryjne i organizacyjne w budowaniu infrastruktury i konfigurowaniu komponentów. Może ono obejmować dodatkowe zmiany organizacyjne, w zależności od tego, jak aktualnie działa organizacja.

W praktyce, rzadko jest to realna opcja dla podmiotów publicznych lub jakiejkolwiek organizacji z istniejącą siecią. Może się jednak zdarzyć, że organizacja zostanie poproszona o wypełnienie nowego obowiązku, który wymagałby zbudowania własnej infrastruktury. W takich przypadkach może być możliwe wprowadzenie w pewnym stopniu koncepcji ZT. Na przykład, urzędowi może zostać powierzona nowa odpowiedzialność, która wiąże się z budową nowej aplikacji, usługi lub bazy danych. Urząd mógłby zaprojektować nową niezbędną infrastrukturę zgodnie z zasadami ZT i bezpiecznej inżynierii systemów [SP8900-160v1], np. ocenić zaufanie podmiotów przed udzieleniem dostępu i ustanowić mikro-obwody bezpieczeństwa wokół nowych zasobów. Stopień powodzenia zależy od tego,

w jakim stopniu ta nowa infrastruktura jest zależna od istniejących zasobów (np. systemów zarządzania identyfikacją).

7.2. HYBRYDOWA ZTA I ARCHITEKTURA BAZUJĄCA NA OBWODZIE

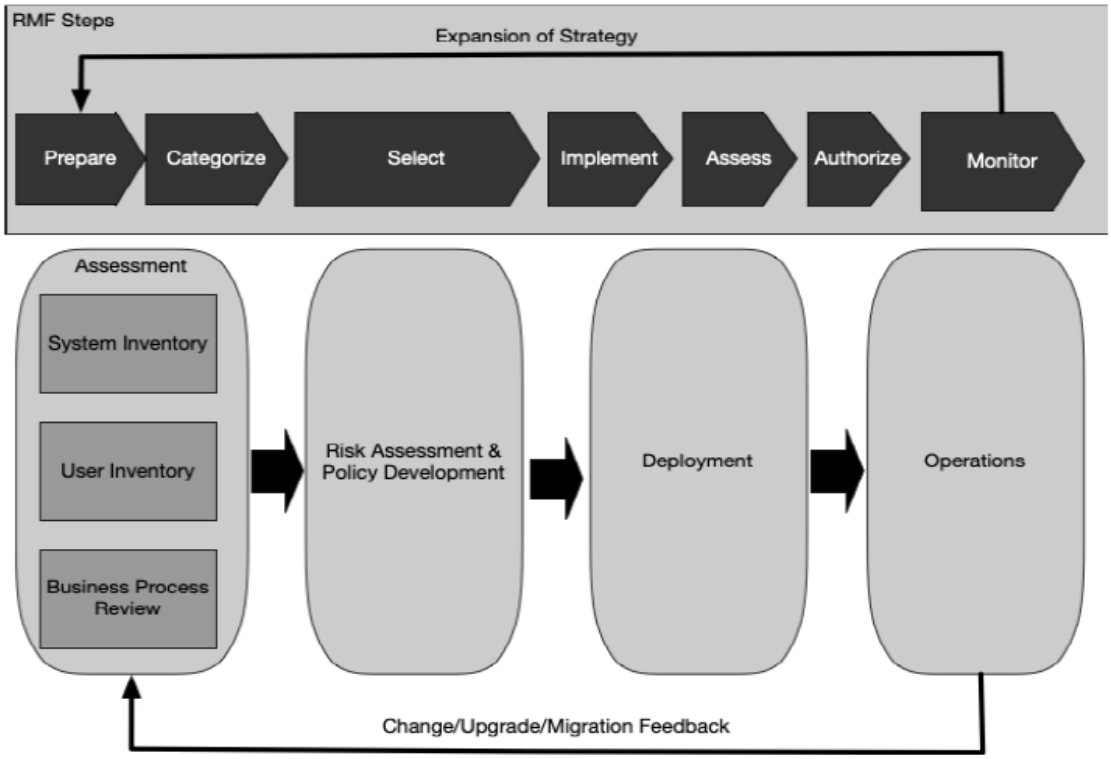
Jest mało prawdopodobne, aby jakakolwiek znacząca organizacja mogła przejść do poziomu zerowego zaufania w jednym cyklu odświeżania technologii. Może istnieć nieokreślony okres czasu, w którym przepływy pracy ZTA w organizacji współistnieją z przepływami pracy niezgodnymi z ZTA. Migracja do podejścia ZTA w organizacji może się odbywać biznesowo proces po procesie. Organizacja musi upewnić się, że wspólne elementy (np. zarządzanie identyfikatorami, zarządzanie urządzeniami, rejestrowanie zdarzeń) są na tyle elastyczne, aby mogły funkcjonować w architekturze zabezpieczeń hybrydowych opartych na ZTA i obwodach bezpieczeństwa. Architekci korporacyjni mogą również ograniczyć rozwiązania kandydujące do ZTA do tych, które mogą współpracować z istniejącymi komponentami.

Migracja istniejącego przepływu pracy do ZTA będzie prawdopodobnie co najmniej wymagała częściowego przeprojektowania. Organizacje mogą skorzystać z tej okazji, aby zastosować praktykę bezpiecznej inżynierii systemowej [SP NIST 800-160 v1], jeżeli jeszcze nie tego zrobiły.

7.3. KROKI W CELU WDROŻENIA ZTA W ISTNIEJĄCEJ ARCHITEKTURZE SIECIOWEJ BAZUJĄCEJ NA OBWODACH

Migracja do ZTA wymaga od organizacji szczegółowej wiedzy na temat swoich aktywów (fizycznych i wirtualnych), podmiotów (w tym uprawnień użytkowników) oraz procesów biznesowych. Wiedza ta jest udostępniana przez ZTA podczas oceny wniosków o dostęp do zasobów. Niepełna wiedza najczęściej prowadzi do niepowodzenia procesu biznesowego, w którym PE zaprzecza żądaniom z powodu niewystarczających informacji. Stanowi to problem zwłaszcza w przypadku nieznanych wdrożeń tzw. "shadow IT" działających w danej organizacji.

Przed podjęciem starań o wprowadzenie ZTA w organizacji, należy przeprowadzić badanie aktywów, podmiotów, przepływów danych i przepływów pracy. Świadomość ta tworzy stan wyjściowy, który musi zostać osiągnięty zanim wdrożenie ZTA będzie możliwe. Organizacja nie może określić, jakie nowe procesy lub systemy muszą zostać wdrożone, jeżeli nie ma wiedzy na temat aktualnego stanu operacji. Badania te mogą być prowadzone równolegle, ale oba są związane z badaniem procesów biznesowych organizacji. Kroki te mogą być odwzorowane w RMF [NSC 800-37], ponieważ każde przyjęcie ZTA jest procesem mającym na celu zmniejszenie ryzyka dla funkcji biznesowych organizacji. Ścieżkę wdrożenia ZTA można zwizualizować na rysunku 12.



Rysunek 12. Cykl wdrażania ZTA.

Po utworzeniu wstępnej inwentaryzacji, następuje regularny cykl utrzymania i aktualizacji. Aktualizacja ta może albo zmienić procesy biznesowe, albo nie mieć żadnego wpływu, ale należy przeprowadzić ocenę procesów biznesowych. Na przykład zmiana dostawcy certyfikatów cyfrowych może nie mieć znaczącego wpływu, ale może obejmować zarządzanie głównym magazynem certyfikatów, monitorowanie dziennika przejrzystości certyfikatów i inne czynniki, które na początku nie są widoczne.

7.3.1. IDENTYFIKACJA UCZESTNIKÓW PRZEDSIĘWZIĘCIA

Aby doprowadzić w organizacji do operacyjnego wdrożenia ZTA, PE musi posiadać wiedzę o podmiotach. Podmioty te mogą obejmować zarówno pracowników, jak i ewentualne NPE, takie jak konta usług, które współdziałają z zasobami.

Użytkownicy o specjalnych uprawnieniach, tacy jak programiści lub administratorzy systemów, wymagają dodatkowej kontroli przy przydzielaniu atrybutów lub ról. W wielu starszych architekturach zabezpieczeń, konta te mogą mieć ogólne uprawnienia do dostępu do wszystkich zasobów organizacji. ZTA powinna zapewnić deweloperom i administratorom wystarczającą elastyczność, aby spełnić ich wymagania biznesowe podczas korzystania z dzienników i działań audytowych w celu identyfikacji wzorców zachowań dostępu. Wdrożenie ZTA może wymagać od administratorów spełnienia bardziej rygorystycznego poziomu zaufania lub kryteriów określonych w NIST SP 800-63A, sekcja 5 [SP800-63A].

7.3.2. IDENTYFIKACJA ZASOBÓW ORGANIZACJI

Jak wspomniano w sekcji 2.1, jednym z kluczowych wymagań ZTA jest zdolność do identyfikacji zasobów i zarządzania nimi. ZTA wymaga również zdolności do identyfikowania i monitorowania urządzeń niebędących własnością organizacji, które mogą znajdować się w jej infrastrukturze sieciowej lub mieć dostęp do jej zasobów. Zdolność do zarządzania zasobami organizacji jest kluczem do pomyślnego wdrożenia ZTA. Obejmuje to komponenty sprzętowe (np. laptopy, telefony, urządzenia IoT) oraz cyfrowe artefakty (np. konta użytkowników, aplikacje, certyfikaty cyfrowe). Przeprowadzenie pełnego spisu wszystkich aktywów organizacji może nie być możliwe, dlatego organizacja powinna rozważyć stworzenie możliwości szybkiej identyfikacji, kategoryzacji i oceny nowo odkrytych aktywów, które znajdują się w jej infrastrukturze.

Wykracza to poza zwykłe katalogowanie i prowadzenie bazy danych zasobów. Obejmuje to również zarządzanie konfiguracją i monitorowanie. Zdolność do obserwowania bieżącego stanu zasobów jest częścią procesu oceny wniosków o dostęp (patrz punkt 2.1). Oznacza to, że organizacja musi być w stanie konfigurować, badać i aktualizować swoje aktywa, takie jak zasoby i kontenery wirtualne. Obejmuje to również zarówno lokalizację fizyczną (oszacowaną jak najdokładniej), jak i lokalizację sieciową. Informacje te powinny informować PE przy podejmowaniu decyzji o dostępie do zasobów.

W miarę możliwości należy również katalogować aktywa niebędące własnością organizacji oraz tzw. "shadow IT" będące jego własnością. Mogą one obejmować wszystko, co jest widoczne dla organizacji (np. adres MAC, lokalizacja w sieci) i rozszerzone poprzez wprowadzenie danych administratora. Informacje te są wykorzystywane nie tylko do podejmowania decyzji o dostępie (ponieważ zasoby współpracowników i BYOD mogą być potrzebne do kontaktowania z PEP), ale także do monitorowania i rejestrowania danych na potrzeby kryminalistyki. „Shadow IT” stanowi szczególny problem, ponieważ zasoby te są własnością organizacji, ale nie są zarządzane jak inne zasoby. Niektóre podejścia ZTA (głównie sieciowe) mogą nawet spowodować, że komponenty „shadow IT” staną się bezużyteczne, ponieważ mogą nie być znane i uwzględnione w zasadach dostępu do sieci.

7.3.3. IDENTYFIKACJA KLUCZOWYCH PROCESÓW I OCENA RYZYKA ZWIĄZANEGO Z PROCESEM ICH REALIZACJI

Trzecia inwentaryzacja, której powinna się podjąć organizacja, to określenie i uszeregowanie procesów biznesowych, przepływów danych i ich relacji w ramach misji. Procesy biznesowe powinny informować o okolicznościach, w których wnioski o dostęp do zasobów są udzielane i odrzucane. Organizacja może zechcieć rozpocząć proces biznesowy niskiego ryzyka przy pierwszym przejściu na ZTA, ponieważ zakłócenia prawdopodobnie nie wpłyną negatywnie

na całą organizację. Po zdobyciu odpowiedniego doświadczenia kandydatami do ZTA mogą stać się procesy bardziej krytyczne.

Często dobrymi kandydatami do ZTA są procesy biznesowe, które wykorzystują zasoby oparte na chmurze lub są wykorzystywane przez pracowników zdalnych i prawdopodobnie da się zauważyć poprawę w zakresie dostępności i bezpieczeństwa. Zamiast projektować obwód bezpieczeństwa organizacji w chmurze lub wprowadzać klientów do sieci korporacyjnej za pośrednictwem sieci VPN, klienci korporacyjni mogą żądać usług w chmurze bezpośrednio. PEP organizacji zapewniają, że zasady organizacji są przestrzegana przed przyznaniem klientowi dostępu do zasobów. Planiści powinni również wziąć pod uwagę potencjalne kompromisy w zakresie wydajności, doświadczenia użytkownika oraz ewentualny wzrost niestabilności przepływu pracy, który może wystąpić podczas wdrażania ZTA dla danego procesu biznesowego.

7.3.4. FORMUŁOWANIE ZASAD KANDYDATURY DO ZTA

Proces identyfikacji usługi lub przepływu pracy jako kandydata do ZTA zależy od kilku czynników: znaczenia procesu dla organizacji, grupy podmiotów, których dotyczy, oraz aktualnego stanu zasobów wykorzystywanych do realizacji przepływu pracy. Wartość zasobu lub przepływu pracy w oparciu o ryzyko dla zasobu lub przepływu pracy można oszacować na podstawie Ram Zarządzania Ryzykiem [NSC 800-37].

Po zidentyfikowaniu składnika aktywów lub przepływu pracy należy zidentyfikować wszystkie zasoby "upstream" (np. systemy zarządzania identyfikatorami, bazy danych, mikrousługi), zasoby "downstream" (np. logowanie, monitorowanie bezpieczeństwa) oraz byty (np. podmioty, konta usług), które są wykorzystywane lub których dotyczy przepływ pracy. Może to mieć wpływ na wybór pierwszego kandydata do migracji do ZTA. Aplikacja/usługa wykorzystywana przez określony podzbiór podmiotów przedsiębiorstwa (np. system zakupów) może być lepsza od tej, która jest istotna dla całej bazy podmiotów organizacji (np. poczty elektronicznej).

Następnie administratorzy organizacji muszą określić zestaw kryteriów (jeżeli stosują pomoc techniczną opartą na kryteriach) lub wagi poziomu zaufania (jeżeli stosują TA oparty na punktacji) dla zasobów wykorzystywanych w procesie biznesowym kandydata (zob. sekcja 3.3.1). Administratorzy mogą być zmuszeni do dostosowania tych kryteriów lub wartości podczas fazy dostrajania. Dostosowania te są konieczne, aby zapewnić skuteczność zasad, ale nie utrudniać dostępu do zasobów.

7.3.5. IDENTYFIKACJA MOŻLIWEGO ROZWIĄZANIA

Po opracowaniu listy kandydujących procesów biznesowych, architekci korporacyjni mogą stworzyć listę możliwych do zastosowania rozwiązań. Niektóre modele wdrożenia (zob.

sekcja 3.1) są lepiej dostosowane do konkretnych przepływów pracy i bieżących ekosystemów organizacji. Podobnie, niektóre rozwiązania oferowane przez producentów są lepiej dostosowane do niektórych przypadków użycia niż inne. Poniżej zaprezentowano niektóre czynniki, które należy rozważyć:

- Czy rozwiązanie wymaga, aby komponenty były instalowane na sprzęcie klienta? Może to ograniczyć procesy biznesowe, w których wykorzystywane lub pożądane są aktywa nie będące własnością organizacji, takie jak BYOD lub współpraca między organizacjami.
- Czy rozwiązanie działa tam, gdzie zasoby procesów biznesowych istnieją w całości na terenie organizacji? Niektóre rozwiązania zakładają, że wymagane zasoby będą znajdowały się w chmurze (tzw. ruch północ-południe, tzn. poza obręb organizacji), a nie w obrębie obwodu organizacji (ruch wschód-zachód, tzn. wewnątrz obwodu organizacji). Lokalizacja kandydujących zasobów procesów biznesowych będzie miała wpływ na możliwe rozwiązania, jak również na ZTA dla procesu.
- Czy rozwiązanie zapewnia możliwość rejestrowania interakcji do analizy? Kluczowym elementem ZT jest zbieranie i wykorzystywanie danych związanych z przepływem procesów, które trafiają z powrotem do PE przy podejmowaniu decyzji o dostępie.
- Czy rozwiązanie zapewnia szerokie wsparcie dla różnych aplikacji, usług i protokołów? Niektóre rozwiązania mogą obsługiwać szeroki zakres protokołów (web, secure shell - SSH itp.) i transportów (IPv4 i IPv6), podczas gdy inne mogą działać tylko w wąskim zakresie, np. web lub email.
- Czy rozwiązanie wymaga zmian w zachowaniu podmiotu? Niektóre rozwiązania mogą wymagać dodatkowych kroków do wykonania danego przepływu pracy. Może to zmienić sposób, w jaki podmioty organizacji wykonują przepływ pracy.

Jednym z rozwiązań jest modelowanie istniejącego procesu biznesowego jako programu pilotażowego, a nie tylko zastępczego. Program pilotażowy może mieć charakter ogólny i dotyczyć kilku procesów biznesowych lub być dostosowany do jednego przypadku zastosowania. Program pilotażowy może być wykorzystany jako "teren testowy" dla ZTA przed przejściem podmiotów do wdrażania ZTA i z dala od dotychczasowej infrastruktury procesów.

7.3.6. WSTĘPNE WDROŻENIE I MONITOROWANIE

Po wybraniu kandydata przepływu pracy i komponentów ZTA można rozpocząć pierwsze wdrożenie. Administratorzy organizacji muszą wdrożyć opracowane zasady przy użyciu wybranych komponentów, ale mogą najpierw chcieć działać w trybie obserwacji i monitorowania. Niewiele zestawów zasad organizacji jest kompletnych w pierwszych

iteracjach: ważnym kontom użytkowników (np. kontom administratorów) można odmówić dostępu do potrzebnych im zasobów lub mogą nie potrzebować wszystkich przyznanych im uprawnień dostępu.

Nowy biznesowy obieg dokumentów ZT może przez pewien czas działać tylko w trybie raportowania, aby upewnić się, że zasady te są skuteczne i wykonalne. Umożliwia to również organizacji zrozumienie podstawowych wniosków o dostęp do aktywów i zasobów, zachowania i wzorców komunikacji. „Wyłącznie raportowanie” oznacza, że dostęp powinien być udzielany dla większości wniosków, a dzienniki i ślady połączeń powinny być porównywane z pierwotnie opracowanymi zasadami. Należy egzekwować i rejestrować podstawowe zasady, takie jak odrzucanie wniosków, które nie spełniają kryteriów MFA lub pochodzą ze znanych, kontrolowanych przez atakującego lub skompromitowanych adresów IP, ale po wstępnym wdrożeniu zasady dostępu powinny być łagodniejsze w celu gromadzenia danych z rzeczywistych interakcji w ramach przepływu pracy ZT. Po ustaleniu podstawowych wzorców aktywności dla przepływu pracy można łatwiej zidentyfikować anormalne zachowania. Jeżeli nie można działać w sposób bardziej łagodny, operatorzy sieci organizacji powinni ściśle monitorować dzienniki i być przygotowani na modyfikację zasad dostępu w oparciu o doświadczenia operacyjne.

7.3.7. ROZSZERZANIE ZTA

Po zdobyciu wystarczającego zaufania i udoskonaleniu zestawu zasad przepływu pracy, organizacja wchodzi w stałą fazę operacyjną. Sieć i aktywa są nadal monitorowane, a ruch jest rejestrowany (zob. sekcja 2.1), ale reakcje i zmiany zasad są dokonywane w niższym tempie, ponieważ nie powinny być znaczące. Podmioty i zainteresowane strony zaangażowane w zasoby i procesy powinny również przekazywać informacje zwrotne w celu usprawnienia działalności. Na tym etapie administratorzy organizacji mogą rozpocząć planowanie kolejnej fazy wdrażania ZT. Podobnie jak w przypadku poprzedniego wdrożenia, należy określić obieg dokumentów i zestaw rozwiązań możliwych do zastosowania oraz opracować wstępne zasady.

Jeżeli jednak nastąpi zmiana w przepływie pracy, należy dokonać ponownej oceny działającej architektury ZT. Znaczące zmiany w systemie - takie jak nowe urządzenia, znaczące aktualizacje oprogramowania (zwłaszcza komponentów logicznych ZT) oraz zmiany w strukturze organizacyjnej - mogą spowodować zmiany w przepływie pracy lub zasadach. W efekcie cały proces powinien być ponownie przemyślany przy założeniu, że część pracy została już wykonana. Na przykład, zakupiono nowe urządzenia, ale nie utworzono nowych kont użytkowników, więc należy zaktualizować tylko inwentaryzację urządzeń.

REFERENCJE

[ACT-IAC] American Council for Technology and Industry Advisory Council (2019) *Zero Trust Cybersecurity Current Trends.* Available at https://www.actiac.org/zero-trust-cybersecurity-current-trends

[Anderson] Anderson B, McGrew D (2017) Machine Learning for Encrypted Malware Traffic Classification: Accounting for Noisy Labels and Non-Stationarity. *Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (ACM, Halifax, Nova Scotia, Canada), pp 1723-1732. https://doi.org/10.1145/3097983.3098163

[BCORE] Department of Defense CIO (2007). Department of Defense Global Information Grid Architecture Vision Version 1.0 June 2007. Available at http://www.acqnotes.com/Attachments/DoD%20GIG%20Architectural%20Vision,%20June%2007.pdf

[CSA-SDP] Cloud Security Alliance (2015) SDP Specification 1.0. Available at https://cloudsecurityalliance.org/artifacts/sdp-specification-v1-0/

[Gilman] Gilman E, Barth D (2017) *Zero Trust Networks: Building Secure Systems in Untrusted Networks* (O'Reilly Media, Inc., Sebastopol, CA), 1st Ed.

[HWAM] Department of Homeland Security (2015) *Hardware Asset Management (HWAM) Capability Description.* Available at https://www.us-cert.gov/sites/default/files/cdm_files/HWAM_CapabilityDescription.pdf

[IBNVN] Cohen R, Barabash K, Rochwerger B, Schour L, Crisan D, Birke R, Minkenberg C, Gusat M, Recio R, Jain V (2013) An Intent-based Approach for Network Virtualization. *2013IFIP/IEEE International Symposium on Integrated Network Management (IM 2013).* (IEEE, Ghent, Belgium), pp 42-50. Available at https://ieeexplore.ieee.org/document/6572968

[JERICHO] The Jericho Forum (2007) *Jericho Forum Commandments,* version 1.2. Available at https://collaboration.opengroup.org/jericho/commandments_v1.2.pdf

Program. (The White House, Washington, DC), OMB Memorandum M-19-03, December 10, 2018. Available at https://www.whitehouse.gov/wp-

[M-19-17] Office of Management and Budget (2019) Enabling Mission Delivery through Improved Identity, Credential, and Access Management. (The White House, Washington, DC), OMB Memorandum M-19-17, May 21, 2019. Available at https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19- 17.pdf

[M-19-19] Office of Management and Budget (2019) Update on Data Center Optimization Initiative (DCOI). (The White House, Washington, DC), OMB Memorandum M-19-19, June 25, 2019. Available at https://datacenters.cio.gov/assets/files/m_19_19.pdf

[M-19-26] Office of Management and Budget (2019) Update to the Trusted Internet Connections (TIC) Initiative. (The White House, Washington, DC), OMB Memorandum M-19-26, September 12, 2019. Available at https://www.whitehouse. gov/wp-content/uploads/2019/09/M- 19-26 pdf

[NISTIR 7987] Ferraiolo DF, Gavrila S, Jansen W (2015) Policy Machine: Features, Architecture, and Specification. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7987, Rev. 1. https://doi.org/10.6028/NIST.IR.7987r1

[NISTIR 8062] Brooks SW, Garcia ME, Lefkovitz NB, Lightman S, Nadeau EM (2017) An Introduction to Privacy Engineering and Risk Management in Federal Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8062. https://doi.org/10.6028/NIST.IR.8062

[NISTPRIV] National Institute of Standards and Technology (2020) Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.01162020

[NSC 199] Standardy kategoryzacji bezpieczeństwa (2021)

[NSC 800-37] Ramy zarządzania ryzykiem w organizacjach i systemach informatycznych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu. (2021)

[SDNBOOK] Nadeau T, Gray K (2013) *SDN: Software Defined Networks: An Authoritative Review of Network Programmability Technologies.* (O’Reilly) 1st Ed.

[SP800-63] Grassi PA, Garcia ME, Fenton JL (2017) Digital Identity Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63-3, Includes updates as of March 2, 2020. https://doi.org/10.6028/NIST.SP.800-63-3

[SP800-63A] Grassi PA, Fenton JL, Lefkovitz NB, Danker JM, Choong Y-Y, Greene KK, Theofanos MF (2017) Digital Identity Guidelines: Enrollment and Identity Proofing. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63A, Includes updates as of March 2, 2020. https://doi.org/10.6028/NIST.SP.800-63A

[SP800-160v1] Ross R, McEvilley M, Oren JC (2016) Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 1, Includes updates as of March 21, 2018. https://doi.org/10.6028/NIST.SP.800-160v1

[SP800-160v2] Ross R, Pillitteri V, Graubart R, Bodeau D, McQuaid R (2019) Developing Cyber Resilient Systems: A Systems Security Engineering Approach. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 2. https://doi.org/10.6028/NIST.SP.800-160v2

[SP800-162] Hu VC, Ferraiolo DF, Kuhn R, Schnitzer A, Sandlin K, Miller R, Scarfone KA (2014) Guide to Attribute Based Access Control (ABAC) Definition and Considerations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-162, Includes updates as of August 2, 2019. https://doi.org/10.6028/NIST.SP.800-162

[SWAM] Department of Homeland Security (2015) *Software Asset Management (SWAM) Capability Description.* Available at https://www.us-cert.gov/sites/default/files/cdm_files/SWAM_CapabilityDescription.pdf

ZAŁĄCZNIK A AKRONIMY

PATRZ: SŁOWNIK KLUCZOWYCH POJĘĆ Z ZASIĘGU CYBERBEZPIECZEŃSTWA NSC 7298

ZAŁĄCZNIK B ZIDENTYFIKOWANE LUKI W OBECNYM STANIE RZECZY W ZTA

Obecna dojrzałość elementów i rozwiązań zerowego zaufania została zbadana w trakcie badań prowadzonych przy opracowywaniu tego dokumentu. Z badań tych wynikało, że obecny stan ekosystemu ZTA nie jest wystarczająco dojrzały do powszechnego przyjęcia. Chociaż możliwe jest wykorzystanie strategii ZTA do planowania i wdrażania środowiska organizacji, nie ma jednego rozwiązania, które zapewniałoby wszystkie niezbędne komponenty. Ponadto, niewiele dostępnych obecnie komponentów ZTA może zostać wykorzystanych we wszystkich procesach pracy obecnych w organizacji.

Poniżej znajduje się podsumowanie zidentyfikowanych luk w ekosystemie ZTA oraz obszarów, które wymagają dalszych badań. Niektóre z tych obszarów mogą znaleźć zastosowanie, ale nie wiadomo, w jaki sposób założenia ZTA zmieniają te obszary, ponieważ nie ma wystarczającego doświadczenia z różnymi środowiskami biznesowymi zorientowanymi na ZTA.

B.1. PRZEGLĄD TECHNOLOGII

Wielu dostawców zostało zaproszonych do przedstawienia swoich produktów i poglądów na temat ZTA. Celem tej ankiety było zidentyfikowanie brakujących elementów, które uniemożliwiają organizacjom przejście na infrastrukturę opartą na zasadzie "zero zaufania" lub utrzymanie istniejącego wdrożenia ZTA. Luki te można podzielić na następujące kategorie: natychmiastowe wdrożenie (natychmiastowe lub krótkoterminowe), luki systemowe, które mają wpływ na utrzymanie lub eksploatację (krótko- lub średnioterminowe), oraz brakująca wiedza (obszary do przyszłych badań). Są one podsumowane w tabeli B-1.

Tabela B- 1. Podsumowanie zidentyfikowanych luk wdrożeniowych

Kategoria	Przykładowe pytania	Zidentyfikowane luki
Natychmiastowe wdrożenie	• Jak należy pisać wymagania dotyczące zamówień publicznych? • W jaki sposób plan ZTA współpracuje z wymaganiami aktualnych przepisów prawa?	• Brak wspólnych ram i słownictwa dla ZTA. • Postrzeganie, że ZTA jest sprzeczna z istniejącą polityką.

Kategoria	Przykładowe pytania	Zidentyfikowane luki
Systemowa	• Jak można zapobiec uzależnieniu się od producenta (vendor lock-in)? • Jak wpływają na siebie różne środowiska ZTA?	• Zbyt duża zależność od API producenta.
Obszary wymagające dalszych badań	• Jak będą się zmieniać zagrożenia w obliczu ZTA? • Jak zmienią się procesy biznesowe w obliczu ZTA?	• Przebieg naruszenia zasad ochrony (udanej kompromitacji) w przedsiębiorstwie wykorzystującym ZTA. • Dokumentowanie doświadczenia użytkownika końcowego w organizacji z ZTA.

B.2. LUKI, KTÓRE UNIEMOŻLIWIAJĄ NATYCHMIASTOWE PRZEJŚCIE DO ZTA

Występują kwestie, które obecnie spowalniają przyjęcie ZTA. Zostały one zaklasyfikowane jako kwestie natychmiastowe i nie należy rozważać możliwości przesunięcia ich obsłużenia w przyszłości. Myśląca przyszłościowo organizacja powinna uznać tą kategorię za kwestię o bezpośrednim znaczeniu dla zapobiegania wstępnemu wdrożeniu komponentów ZTA, ale kwestie stanowią osobną kategorię w niniejszej analizie.

B.2.1. BRAK OGÓLNYCH WYTYCZNYCH W ZAKRESIE PROJEKTOWANIA, PLANOWANIA I ZAMÓWIEŃ DOTYCZĄCYCH ZTA

„Zerowe zaufanie” jako strategia projektowania i wdrażania infrastruktury korporacyjnej jest nadal koncepcją formalną. Branża nie skupiła się jeszcze wokół jednego zestawu wytycznych lub koncepcji opisujących komponenty i działanie ZTA. Utrudnia to organizacjom (np. urzędom państwowym) opracowanie spójnych wymagań i zasad w zakresie projektowania infrastruktury organizacji i zamawiania komponentów.

Motywem przewodnim dla sekcji 2.1 i 3.1 jest próba stworzenia neutralnej bazy wytycznych i koncepcji do opisu ZTA. Opracowano abstrakcyjne komponenty ZTA i modele wdrożeniowe, które mają służyć jako podstawowe wytyczne i sposoby myślenia o ZTA. Celem jest zapewnienie wspólnego sposobu postrzegania, modelowania i omawiania rozwiązań ZTA

podczas opracowywania wymagań organizacji i przeprowadzania badań rynkowych. Powyższe rozdziały mogą okazać się niekompletne, ponieważ brakuje doświadczeń z ZTA w urzędach państwowych, ale mogą one służyć jako podstawa rozważań dla wspólnych ram koncepcyjnych.

B.2.2. POSTRZEGANIE, ŻE ZTA STANOWI KONFLIKT Z ISTNIEJĄCYMI ZASADAMI CYBERBEZPIECZEŃSTWA

Istnieje błędne przekonanie, że ZTA stanowi pojedyncze podejście z zestawem rozwiązań, które są niezgodne z istniejącym poglądem na cyberbezpieczeństwo. „Zerowe zaufanie" powinno być natomiast postrzegane jako ewolucja obecnych strategii cyberbezpieczeństwa, ponieważ od dłuższego czasu wiele koncepcji i pomysłów krąży wokół takiego podejścia. Zachęca się urzędy państwowe do przyjęcia podejścia do cyberbezpieczeństwa opartego na zasadzie zerowego zaufania w ramach istniejących wytycznych (zob. sekcja 6[10]). Jeżeli dany urząd posiada dojrzały system zarządzania identyfikacją i solidne możliwości w zakresie CDM, jest na drodze do wprowadzenia ZTA (zob. sekcja 7.3). Luka ta wynika z błędnego pojmowania ZTA i jego ewolucji w stosunku do poprzednich paradygmatów cyberbezpieczeństwa.

B.3. LUKI SYSTEMOWE, KTÓRE WPŁYWAJĄ NA ZTA

Są to luki, które mają wpływ na początkowe wdrożenie ZTA oraz dalszą jego eksploatację i dojrzałość. Luki te mogą spowolnić przyjęcie ZTA w urzędach lub doprowadzić do rozdrobnienia branży komponentów ZTA. Luki systemowe to obszary, w których pomocne mogą być otwarte standardy (opracowane przez organizację opracowującą normy (*ang. standards development organization - SDO*] lub konsorcjum branżowe).

B.3.1. STANDARYZACJA INTERFEJSÓW MIĘDZY KOMPONENTAMI

Podczas przeglądu technologii okazało się, że żaden z dostawców nie oferuje całościowego rozwiązania, które zapewniłoby „zerowe zaufanie". Ponadto, niepożądane jest korzystanie z rozwiązania jednego dostawcy w celu osiągnięcia zerowego zaufania, albowiem może to powodować ryzyko zablokowania przez dostawcę (*ang. vendor lock-in*). Wymagana jest zatem interoperacyjności komponentów nie tylko w momencie zakupu, ale również na przestrzeni czasu.

Spektrum komponentów w ramach dostawców jest ogromne, przy czym wiele produktów koncentruje się na jednej niszy w ramach rozwiązania "zero zaufania" i polega na innych produktach, które dostarczają dane lub świadczą jakieś usługi na rzecz innego komponentu (np. integracja MFA w zakresie dostępu do zasobów). Aby osiągnąć tą integrację dostawcy zbyt często stosują zastrzeżone API dostarczane przez firmy partnerskie, a nie API bazujące na otwartych standardach. Problem z tym podejściem polega na tym, że te API są

[10] W polskiej wersji Rozdział 6 został pominięty, jako odnoszący się do systemu prawnego USA

własnościowe i kontrolowane przez jednego dostawcę. Dostawca kontrolujący może zmienić zachowanie API, a integratorzy w odpowiedzi na to są zmuszani do aktualizacji swoich produktów. Wymaga to ścisłej współpracy pomiędzy społecznościami sprzedawców w celu zapewnienia wczesnego powiadamiania o modyfikacjach w obrębie interfejsów API, które mogą mieć wpływ na kompatybilność produktów. Stanowi to dodatkowe obciążenie dla sprzedawców i konsumentów: dostawcy muszą przeznaczać zasoby na zmianę swoich produktów, a konsumenci muszą stosować aktualizacje do wielu produktów, gdy jeden ze sprzedawców wprowadza zmiany do swojego zastrzeżonego interfejsu API. Dodatkowo, dostawcy są zobowiązani do wdrożenia i utrzymania zabezpieczeń dla każdego komponentu partnera, aby zapewnić maksymalną kompatybilność i interoperacyjność. Na przykład wielu dostawców produktów MFA musi tworzyć różne klasy zabezpieczeń dla każdego dostawcy usług w chmurze lub systemu zarządzania tożsamością, tak aby można je było stosować u różnych klientów.

Po stronie klienta generuje to dodatkowe problemy podczas opracowywania wymagań dotyczących zakupu produktów. Nie ma standardów, na których nabywcy mogliby by się powoływać przy określaniu kompatybilności pomiędzy produktami. Dlatego też bardzo trudno jest stworzyć wieloletni harmonogram przejścia na ZTA, ponieważ nie jest możliwe określenie minimalnego zestawu wymagań dotyczących kompatybilności komponentów.

B.3.2. POJAWIAJĄCE SIĘ STANDARDY, KTÓRE ROZWIĄZUJĄ PROBLEM NADMIERNEGO POLEGANIA NA ZASTRZEŻONYCH INTERFEJSACH API

Ponieważ nie ma jednego rozwiązania dla opracowania ZTA, nie ma jednego zestawu narzędzi lub usług dla „zero zaufania” u przedsiębiorcy. W związku z tym nie jest możliwe posiadanie jednego protokołu lub specyfikacji, które umożliwiłby organizacji przejście na ZTA. Obecnie istnieje szeroka gama modeli i rozwiązań, które starają stać się wiodącymi w odniesieniu do ZTA.

Oznacza to, że istnieje potrzeba opracowania zestawu otwartych, standardowych protokołów lub ram, które pomogą organizacjom w migracji do ZTA. SDO, takie jak Internet Engineering Task Force (IETF), mają określone protokoły, które mogą być przydatne w wymianie informacji o zagrożeniach (zwane XMPP-Grid [1]). Cloud Security Alliance (CSA) opracował specyfikację dla Software Defined Perimeter (SDP) [2], który może być również przydatny w ZTA. Wysiłki powinny być skierowane na zbadanie aktualnego stanu specyfikacji związanych z ZTA lub protokołów niezbędnych dla stworzenia użytecznego ZTA oraz na określenie miejsc, w których konieczne są prace nad stworzeniem lub ulepszeniem tych specyfikacji.

B.4. LUKI W WIEDZY W ZTA I PRZYSZŁE OBSZARY BADAŃ

Wymienione tu luki nie utrudniają organizacji przyjęcia ZTA. Są to szare obszary w wiedzy na temat operacyjnych środowisk ZTA, a większość z nich wynika z braku czasu i doświadczenia z dojrzałymi wdrożeniami typu „zero zaufania". Są to obszary przyszłej pracy dla naukowców.

B.4.1. ODPOWIEDŹ ATAKUJĄCYCH NA ZTA

Prawidłowo wdrożona w organizacji ZTA wpłynie na poprawę jej stanu cyberbezpieczeństwa w stosunku do tradycyjnego zabezpieczenia opartego na ochronie obwodowej. ZTA ma na celu zmniejszenie narażenia zasobów na atak i zminimalizowanie lub zapobieżenie bocznym ruchom w obrębie organizacji w przypadku ataku z wewnątrz.

Jednak zdeterminowani napastnicy nie będą siedzieć bezczynnie, a zamiast tego zmienią zachowanie w obliczu ZTA. Otwartą kwestią jest to, jak zmienią się ataki. Jedną z możliwości jest to, że ataki mające na celu kradzież danych uwierzytelniających zostaną rozszerzone na docelowe MFA (np. phishing, inżynieria społeczna). Inną możliwością jest to, że w rozwiązaniu hybrydowym opartym na ZTA/obwodzie, atakujący skoncentrują się na procesach biznesowych, w których nie zastosowano zasad ZTA (tzn. podążają za tradycyjnymi zabezpieczeniami opartymi na obwodzie sieci), próbując uzyskać pewną pozycję w procesie biznesowym ZTA.

W miarę jak ZTA będzie dojrzewać, widać będzie więcej wdrożeń i zdobywać się będzie doświadczenie, co spowoduje, że skuteczność ZTA w zmniejszaniu powierzchni ataku zasobów może stać się oczywista. Konieczne będzie również opracowanie mierników sukcesu ZTA w stosunku do starszych strategii cyberbezpieczeństwa.

B.4.2. DOŚWIADCZENIE UŻYTKOWNIKÓW W ŚRODOWISKU ZTA

Dotychczas nie przeprowadzono rygorystycznego badania sposobu działania użytkowników końcowych w organizacji korzystającej z ZTA. Wynika to głównie z braku dostępnych do analizy dużych przypadków użycia ZTA. Przeprowadzono jednak badania dotyczące reakcji użytkowników MFA i innych operacji związanych z bezpieczeństwem, które są częścią organizacji korzystającej z ZTA. Prace te mogą stanowić podstawę do przewidywania doświadczeń i zachowań użytkowników końcowych podczas korzystania z przepływów pracy ZTA.

Jednym z zestawów badań, które mogą przewidzieć, w jaki sposób ZTA wpływa na doświadczenia użytkowników końcowych, jest praca wykonana na temat korzystania z urządzeń wielofunkcyjnych w organizacjach i tzw. „zmęczenia bezpieczeństwem". Zmęczenie bezpieczeństwem [3] jest zjawiskiem, w którym użytkownicy końcowi stają w obliczu tak wielu zasad i problemów związanych z bezpieczeństwem, że zaczyna ono wpływać negatywnie na ich wydajność. Inne badania pokazują, że urządzenia wielofunkcyjne mogą zmieniać zachowanie użytkowników, ale ogólna zmiana jest zróżnicowana [4] [5].

Niektórzy użytkownicy chętnie akceptują MFA, jeśli proces jest usprawniony i obejmuje urządzenia, których są przyzwyczajeni używać lub mieć przy sobie (np. aplikacje na smartfony). Niektórzy użytkownicy sprzeciwiają się jednak używaniu urządzeń będących ich własnością do procesów biznesowych lub mają poczucie, że są stale monitorowani pod kątem ewentualnych naruszeń zasad IT.

B.4.3. ODPORNOŚĆ ZTA NA ZAKŁÓCENIA W FUNKCJONOWANIU ORGANIZACJI I SIECI

Badanie ekosystemu dostawców ZTA pokazało szeroki zakres infrastruktury, którą organizacja wdrażająca ZTA musiałaby rozważyć. Jak wcześniej zauważono, nie ma obecnie jednego dostawcy całościowego rozwiązania „zero zaufania". W rezultacie organizacje będą kupować kilka różnych usług i produktów, co może prowadzić do powstania sieci zależności dla komponentów. Jeżeli jeden istotny komponent zostanie zakłócony lub będzie nieosiągalny, może dojść do kaskady awarii, które będą miały wpływ na jeden lub wiele procesów biznesowych.

Większość badanych produktów i usług opierała się na obecności chmury w celu zapewnienia odporności, ale nawet usługi w chmurze mogą się stać niedostępne w wyniku ataku lub zwykłego błędu. Kiedy to nastąpi, kluczowe komponenty wykorzystywane do podejmowania decyzji o dostępie mogą być nieosiągalne lub mogą nie być w stanie komunikować się z innymi komponentami. Na przykład, mimo że komponenty PE i PA znajdujące się w chmurze będą osiągalne podczas rozproszonego ataku DDoS (Distributed Denial-of-service), ale mogą nie być w stanie dotrzeć do wszystkich PEP znajdujących się w zasobach. Potrzebne są badania nad identyfikacją możliwych wąskich gardeł w modelach wdrażania ZTA i ich wpływu na działanie sieci w sytuacji, gdy komponent ZTA jest nieosiągalny lub ma ograniczoną dostępność.

Plany dotyczące ciągłości działania (*ang. continuity of operations plans - COOP*) organizacji będą prawdopodobnie wymagały rewizji przy przyjmowaniu ZTA. ZTA ułatwia wiele aspektów COOP, ponieważ pracownicy zdalni mogą mieć taki sam dostęp do zasobów, jaki mieli w siedzibie. Jednak zasady takie jak MFA mogą mieć również negatywny wpływ, o ile użytkownicy nie są odpowiednio przeszkoleni lub nie mają doświadczenia. Użytkownicy mogą zapomnieć lub nie mieć dostępu do tokenów i urządzeń korporacyjnych w sytuacjach awaryjnych, co wpłynie na szybkość i efektywność procesów biznesowych organizacji.

B.5. REFERENCJE

[1] Cam-Winget N (ed.), Appala S, Pope S, Saint-Andre P (2019) Using Extensible Messaging and Presence Protocol (XMPP) for Security Information Exchange. (Internet Engineering Task Force (IETF)), IETF Request for Comments (RFC) 8600. https://doi.org/10.17487/RFC8600

[2] Software Defined Perimeter Working Group "SDP Specification 1.0" Cloud Security Alliance. April 2014.

[3] Stanton B, Theofanos MF, Spickard Prettyman S, Furman S (2016) Security Fatigue. *IT Professional* 18(5):26-32. https://doi.org/10.1109/MITP.2016.84

[4] Strouble D, Shechtman GM, Alsop AS (2009) Productivity and Usability Effects of Using a Two-Factor Security System. *SAIS 2009 Proceedings* (AIS, Charleston, SC), p 37. Available at http://aisel.aisnet.org/sais2009/37

[5] Weidman J, Grossklags J (2017) I Like It but I Hate It: Employee Perceptions Towards an Institutional Transition to BYOD Second-Factor Authentication. *Proceedings of the 33rd Annual Computer Security Applications Conference (ACSAC 2017)* (ACM, Orlando, FL), pp 212-224. https://doi.org/10.1145/3134600.3134629