Kancelaria Prezesa
Rady Ministrów

NARODOWY STANDARD CYBERBEZPIECZEŃSTWA
NSC 800-210 wer. 1.0

21 grudnia 2022

Ogólne wytyczne dotyczące kontroli dostępu do systemów chmury obliczeniowej

Publikacja dostępna pod adresem:

Narodowe Standardy Cyberbezpieczeństwa

DEPARTAMENT CYBERBEZPIECZEŃSTWA

PREAMBUŁA

Szanowni Państwo,

oddajemy w Państwa ręce zestaw publikacji specjalnych - Narodowe Standardy Cyberbezpieczeństwa, o których mowa w interwencji 2.1 celu szczegółowego 2 Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024, *Opracowanie i wdrożenie Narodowych Standardów Cyberbezpieczeństwa oraz promowanie dobrych praktyk i zaleceń*. Standardy zostały opracowane na podstawie publikacji amerykańskiego National Institute of Science and Technology (NIST) i posiadają mapowanie na obowiązujące w polskim systemie prawnym Polskie Normy, na których oparte jest zarządzanie bezpieczeństwem informacji w podmiotach krajowego systemu cyberbezpieczeństwa.

Standardy stanowią przewodniki metodyczne, które ułatwiają zbudowanie efektywnego systemu zarządzania bezpieczeństwem informacji w oparciu o praktykę stosowaną w tym zakresie w administracji federalnej USA.

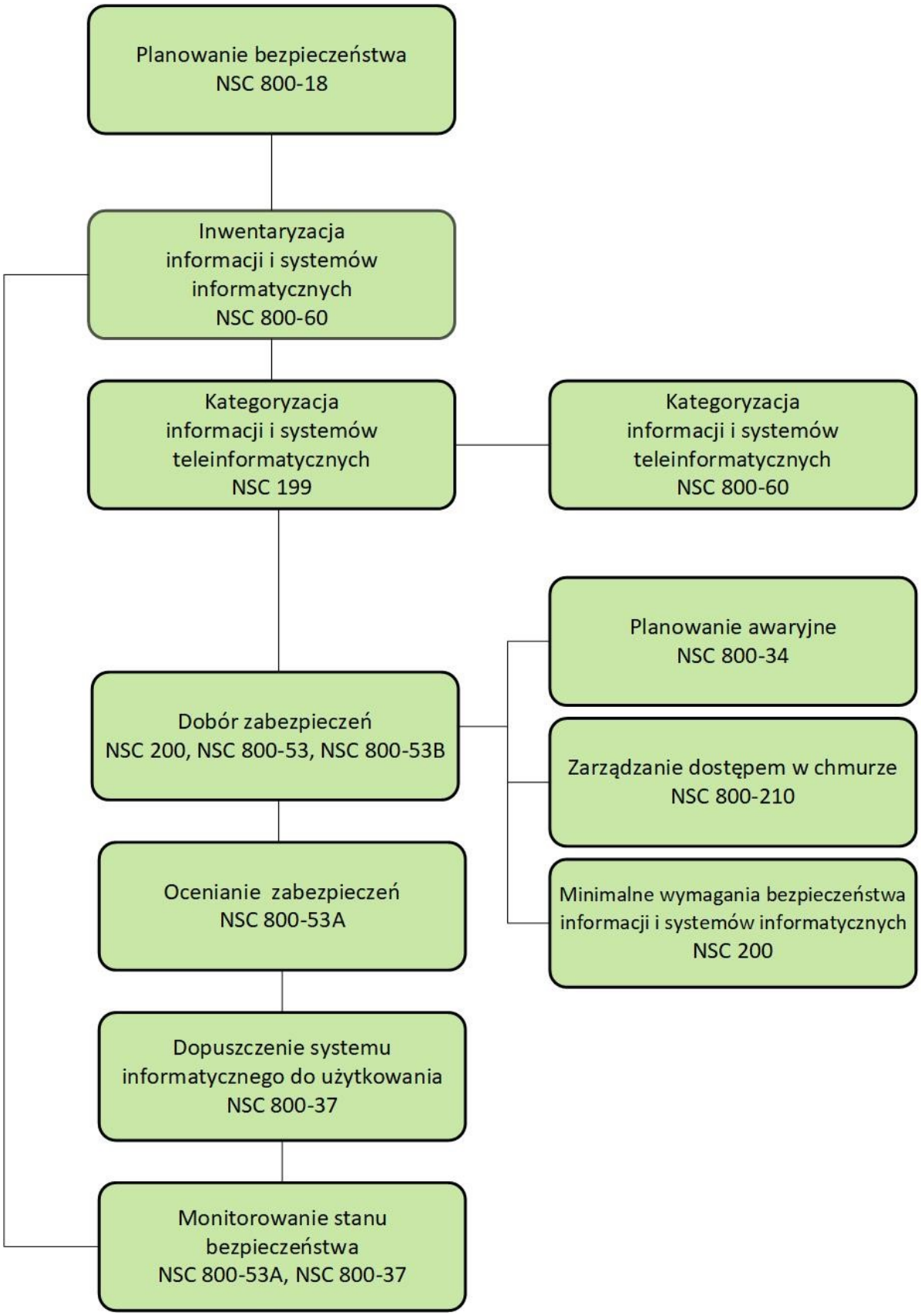
Zestaw publikacji specjalnych obejmuje następujące pozycje:

- NSC 199, Standardy kategoryzacji bezpieczeństwa – na podstawie FIPS 199.
- NSC 200, Minimalne wymagania bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych – na podstawie FIPS 200.
- NSC 800-18, Przewodnik do opracowywania planów bezpieczeństwa systemów informacyjnych w podmiotach publicznych – na podstawie NIST SP 800-18.
- NSC 800-30, Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne – na podstawie NIST SP 800-30.
- NSC 800-34, Poradnik planowania awaryjnego – na podstawie NIST SP 800-34.
- NSC 800-37, Ramy zarządzania ryzykiem w organizacjach i systemach informacyjnych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu – na podstawie NIST SP 800-37.
- NSC 800-39, Zarządzanie ryzykiem bezpieczeństwa informacji. Przegląd struktury organizacyjnej, misji i systemu informacyjnego – na podstawie NIST SP 800-39.

- NSC 800-53, Zabezpieczenia i ochrona prywatności systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53.
- NSC 800-53A, Ocenianie środków bezpieczeństwa i ochrony prywatności systemów informacyjnych oraz organizacji. Tworzenie skutecznych planów oceny – na podstawie NIST SP 800-53A.
- NSC 800-53B, Zabezpieczenia bazowe systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53B.
- NSC 800-60, Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informacyjnego – na podstawie NIST SP 800-60.
- NSC 800-61, Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego – na podstawie NIST SP 800-61.
- NSC 800-210, Ogólne wytyczne dotyczące kontroli dostępu do systemów chmury obliczeniowej – na podstawie NIST SP 800-210.

W oparciu o te publikacje można stosunkowo łatwo zbudować system zarządzania bezpieczeństwem informacji i sprawować nad nim niezbędną kontrolę.

Cykl zarządzania bezpieczeństwem informacji bazujący na publikacjach NIST wykorzystuje następujące dokumenty:



Cykl zarządzania bezpieczeństwem informacji

WSPÓLNE FUNDAMENTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

National Institute of Standards and Technology (NIST) opracował szereg standardów i wytycznych w celu zapewnienia jednolitego podejścia do problematyki bezpieczeństwa informacji i systemów informacyjnych administracji federalnej USA. Podstawową rolę w podejściu do zagadnień związanych z zapewnieniem bezpieczeństwa informacji i systemów informacyjnych oraz ochrony prywatności odgrywa elastyczny i spójny sposób zarządzania ryzykiem związanym z bezpieczeństwem i prywatnością działalności i majątku organizacji, osób fizycznych i państwa. Zarządzanie ryzykiem stanowi podstawę do wdrożenia stosownych zabezpieczeń w systemach informacyjnych, ocenę tych zabezpieczeń, wzajemną akceptację dowodów oceny bezpieczeństwa i ochrony prywatności oraz decyzji autoryzacyjnych. Dzięki jednolitemu podejściu do zarządzania ryzykiem ułatwia także wymianę informacji i współpracę pomiędzy różnymi podmiotami.

NIST kontynuuje współpracę z sektorem publicznym i prywatnym w celu stworzenia map i relacji pomiędzy opracowanymi przez siebie standardami i wytycznymi, a tymi, które zostały opracowane przez inne organizacje (m. in. ISO[1]), co zapewnia zgodność w przypadku, gdy regulacje wymagają stosowania tych innych standardów.

Publikacje NIST co do zasady nie są objęte restrykcjami wynikającymi z autorskich praw majątkowych. Są powszechnie dostępne oraz dopuszczone do użytku poza administracją federalną USA. Charakteryzują się pragmatycznym podejściem do zagadnień związanych z bezpieczeństwem informacji i systemów informacyjnych oraz ochrony prywatności, przez co ułatwiają podmiotom opracowanie i eksploatację systemu zarządzania tym bezpieczeństwem.

Biorąc pod uwagę wszystkie powyższe aspekty, autorzy niniejszej publikacji polecają opracowania NIST, jako godne zaufania i rekomendują stosowanie ich przez polskie

[1] International Organization for Standardization (ISO) - Międzynarodowa Organizacja Normalizacyjna– organizacja pozarządowa zrzeszająca krajowe organizacje normalizacyjne.

podmioty przy opracowywaniu systemów zarządzania bezpieczeństwem informacji, wdrażaniu zabezpieczeń i ocenie ich działania.

Podmioty, urządzenia lub materiały prezentowane są w niniejszym dokumencie w celu odpowiedniego opisania procedury lub koncepcji eksperymentalnej. Celem ich wskazania nie jest nakłanianie do korzystania z ww. podmiotów, urządzeń lub materiałów lub ich poparcie. Wskazanie ich nie ma również na celu sugerowania, że te podmioty, materiały lub sprzęt są najlepsze z dostępnych w danej dziedzinie.

W niniejszej publikacji mogą znajdować się odniesienia do innych opracowywanych przez nas publikacji. Informacje tu zawarte, w tym koncepcje, praktyki i metodologie, mogą być wykorzystywane przez organizacje jeszcze przed ukończeniem innych towarzyszących temu standardowi publikacji. W związku z tym, do czasu ukończenia każdej publikacji powinny obowiązywać dotychczasowe wymagania, wytyczne i procedury, jeśli takie istnieją. W ramach planowanych przez Państwa prac zalecamy śledzenie naszych prac publikacyjnych.

Aktualne informacje o prowadzonych przez nas pracach dostępne są pod adresem:

 Narodowe Standardy Cyberbezpieczeństwa

Jesteśmy również otwarci na wszelkie Państwa sugestie, które pomogą nam w dalszych pracach nad standardami cyberbezpieczeństwa i zachęcamy do kontaktu.

 +48222455922

 sekretariat.dc@mc.gov.pl

Niniejsza publikacja NSC 800-210, ***Ogólne wytyczne dotyczące kontroli dostępu do systemów chmury obliczeniowej***, opracowana została za zgodą National Institute of Science and Technology (NIST), na podstawie specjalnej publikacji NIST SP 800-210, *General Access Control Guidance for Cloud Systems*.
Terminologia angielska i akronimy występujące w publikacji zdefiniowane są w dokumencie NSC 7298, *Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa*.

Spis treści

Spis ilustracji

Spis tabel

PODSUMOWANIE ZARZĄDCZE

Systemy chmur obliczeniowych zostały opracowane na przestrzeni czasu w oparciu o połączenie programów (aplikacji), komponentów sprzętowych i technologii wirtualizacji. Cechy charakterystyczne chmury, takie jak łączenie zasobów, szybka elastyczność i usługi typu „płać, jeśli używasz" (*ang. pay-as-you-go*), przyspieszyły ich szerokie zastosowanie przez przedsiębiorców, administrację publiczną i środowiska akademickie. W szczególności, systemy chmur oferują usługi aplikacyjne, przechowywanie danych, zarządzanie danymi, tworzenie sieci oraz zarządzanie zasobami obliczeniowymi dla konsumentów na poziomie sieci (przez Internet). Pomimo dużych postępów w zakresie systemów chmurowych, zgłaszane są obawy dotyczące oferowanego poziomu bezpieczeństwa i prywatności. Znaczenie tych obaw staje się bardziej widoczne, gdy weźmie się pod uwagę ogromną liczbę użytkowników, którzy przyjęli usługi w chmurze.

Niniejszy dokument przedstawia charakterystykę kontroli dostępu w chmurze (*ang. access control - AC*)[2] oraz zestaw ogólnych wytycznych kontroli dostępu dla dostępnych modeli usług w chmurze - *IaaS* (infrastruktura jako usługa), *PaaS* (platforma jako usługa) oraz *SaaS* (oprogramowanie jako usługa) - bez uwzględnienia modeli wdrożeniowych (np. chmura publiczna, chmura prywatna), które wymagają innej warstwy kontroli dostępu, zależnej od wymogów bezpieczeństwa funkcji biznesowej podmiotu wdrażającego system w chmurze. W różnych modelach świadczenia usług należy rozważyć zarządzanie różnymi rodzajami dostępu do oferowanych komponentów usług. Takie rozważania mogą mieć charakter hierarchiczny, np. w jaki sposób zasady kontroli dostępu komponentów funkcjonalnych w modelu usług niższego poziomu (np. warstwy sieciowej i pamięci masowej w modelu IaaS) mają zastosowanie w tych samych komponentach funkcjonalnych w modelu usług wyższego poziomu (np. warstwy sieciowej i pamięci masowej w modelach PaaS i SaaS). Ogólnie rzecz biorąc, zasady kontroli dostępu w przypadku IaaS mają również zastosowanie do PaaS i SaaS, a zasady

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

kontroli dostępu w przypadku IaaS i PaaS mają również zastosowanie do SaaS. W związku z tym wytyczne AC dotyczące IaaS mają zastosowanie do PaaS i SaaS, a wytyczne AC dotyczące IaaS i PaaS mają również zastosowanie do SaaS. Jednakże każdy model usługi ma swoje własne ukierunkowanie w odniesieniu do wymogów dotyczących kontroli dostępu do jego usług.

1. WSTĘP

1.1. CEL

Kontrola dostępu (AC) w celu ochrony wrażliwych danych i krytycznych zasobów obliczeniowych w chmurze określa sposób, w jaki zleceniodawcy (tj. użytkownicy i procesy) mogą uzyskać dostęp do zasobów w oparciu o określone zasady AC. Biorąc pod uwagę heterogeniczność i zdalny charakter modeli usług w chmurze, należy ponownie przeanalizować AC i jego ogólne pojęcia. W ostatnich latach wiele prac koncentrowało się na AC w systemach chmurowych. Są to jednak przede wszystkim rozwiązania ad hoc ukierunkowane na konkretne aplikacje w chmurze i nie zapewniają kompleksowego spojrzenia na AC w chmurze.

Modele wdrażania chmury (np. chmura publiczna, chmura prywatna, chmura wspólnotowa, chmura hybrydowa itp.) są konfigurowane w zależności od użytkowników chmury, zakresu usług i zasobów w oparciu o wymagania usługowe. Niniejszy dokument przedstawia zestaw ogólnych wytycznych AC dla modeli usług w chmurze niezależnych od jej modeli wdrożeniowych, ponieważ wymaga innej warstwy kontroli dostępu, która zależy od wymogów bezpieczeństwa funkcji biznesowej, do której wykorzystywany jest system chmury. Jak pokazano na rysunku 3, różne modele usług wymagają zarządzania różnymi rodzajami dostępu do komponentów oferowanej usługi. Ponieważ takie modele usług można uznać za hierarchiczne, względy AC dotyczące komponentów funkcjonalnych w modelu usług niższego poziomu (zgodnie z rysunkiem 2) modele systemowe (np. warstwy sieciowe i pamięci masowej w modelu IaaS) mają również zastosowanie do tych samych komponentów funkcjonalnych w modelu usług wyższego poziomu (np. warstwy sieciowe i pamięci masowej w modelach PaaS i SaaS). Ogólnie rzecz biorąc, względy AC dla IaaS mają również zastosowanie do PaaS i SaaS, a względy AC dla IaaS i PaaS mają również zastosowanie do SaaS. Zatem wytyczne AC dla IaaS mają zastosowanie do PaaS i SaaS, a wytyczne AC dla IaaS i PaaS mają również zastosowanie do SaaS. Jednak każdy model usługi ma swoje własne ukierunkowanie w odniesieniu do AC. Na przykład dostawca IaaS może włożyć więcej wysiłku w kontrolę wirtualizacji,

natomiast dostawca SaaS oprócz kontroli wirtualizacji musi uwzględnić bezpieczeństwo danych i prywatność świadczonych przez siebie usług.

1.2. ZAKRES

Niniejszy dokument koncentruje się na dostarczeniu wskazówek dotyczących systemów kontroli dostępu, które są stosowane przez organizację w implementacji chmury. Nie określa on wewnętrznych standardów kontroli dostępu do chmury, które organizacja może stosować w swoich systemach lub w ramach społeczności innej niż sam podmiot[3].

1.3. ODBIORCY

Adresatem tego dokumentu jest podmiot, który wdraża rozwiązania kontroli dostępu do informacji w systemach chmurowych. Niniejszy dokument zakłada, że czytelnicy znają systemy chmury i kontroli dostępu (autoryzacji) oraz posiadają podstawową wiedzę na temat systemów operacyjnych, baz danych, sieci i bezpieczeństwa. Biorąc pod uwagę stale zmieniający się charakter branży informatycznej (IT), czytelnicy w celu uzyskania bardziej aktualnych i szczegółowych informacji są zdecydowanie zachęcani do korzystania z innych dokumentów - w tym wymienionych w referencjach zawartych w niniejszym opracowaniu.

1.4. STRUKTURA DOKUMENTU

Dokument zawiera następujące rozdziały i załączniki:

- W rozdziale 1 określono cel i zakres kontroli dostępu w odniesieniu do systemów chmury obliczeniowej.
- Rozdział 2 zawiera przegląd charakterystyki kontroli dostępu do chmury.
- W rozdziale 3 omówiono wytyczne dotyczące systemów kontroli dostępu dla IaaS (infrastruktura jako usługa).

[3] W dokumencie słowo *podmiot* jest wymiennie stosowane z wyrazem *organizacja*.

- W rozdziale 4 omówiono wytyczne dotyczące systemów kontroli dostępu dla PaaS (platforma jako usługa).
- W rozdziale 5 omówiono wytyczne dotyczące systemów kontroli dostępu dla SaaS (oprogramowanie jako usługa).
- W rozdziale 6 omówiono wytyczne dotyczące operacji na zewnątrz i wewnątrz chmury.
- Rozdział 7 podsumowuje dokument z podaniem przyszłych kierunków.

2. CHARAKTERYSTYKA KONTROLI DOSTĘPU W ROZWIĄZANIACH CHMUROWYCH

Dzięki wsparciu różnych modeli usług, systemy chmurowe mogą zapewnić szeroki zakres usług swoim użytkownikom końcowym, programistom i administratorom systemów. Systemy w chmurze zostały opracowane na przestrzeni wielu lat w oparciu o połączenie oprogramowania, komponentów sprzętowych i technologii wirtualizacji. Cechy charakterystyczne chmury, takie jak łączenie zasobów, szybka elastyczność i odpłatność za faktyczne użycie usług, przyspieszyły jej szerokie zastosowanie przez przedsiębiorców, podmioty publiczne i środowiska akademickie. W szczególności, systemy chmury oferują usługi aplikacyjne, przechowywanie danych, zarządzanie danymi, sieci oraz zarządzanie zasobami obliczeniowymi dla odbiorców usług chmurowych[4] za pośrednictwem sieci (w szczególności Internetu). Przykładami popularnych aplikacji w chmurze są internetowe usługi poczty elektronicznej (np. Gmail Google, Microsoft Office 365 Outlook), przechowywanie danych użytkowników końcowych (np. Google Drive, Microsoft OneDrive, Dropbox) oraz zarządzanie relacjami z klientami i systemami inteligencji biznesowej do zarządzania przedsiębiorstwem (np. CRM Cloud, Workday). Pomimo ogromnego rozwoju systemów chmurowych, pojawiły się obawy o oferowane poziomy bezpieczeństwa i poziomy ochrony prywatności. Znaczenie tych obaw staje się bardziej widoczne, gdy weźmiemy pod uwagę ogromną liczbę użytkowników, którzy wykorzystują usługi w chmurze [1][5].

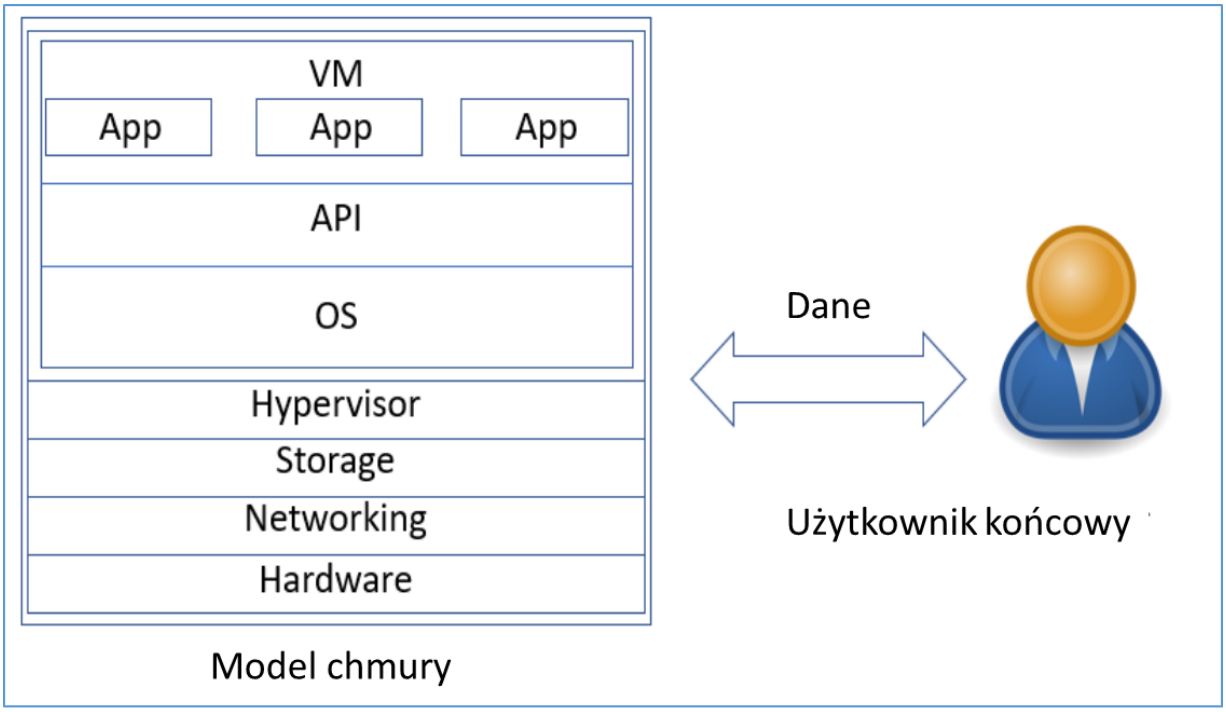
Według słownika NSC-7298, przetwarzanie w chmurze (*ang. cloud computing*) jest zdefiniowane, jako "model umożliwiający powszechny, łatwy i wygodny dostęp

[4] Odbiorcy usług chmurowych odgrywają różnorodne role w wykorzystywaniu usług w chmurze, np. planiści systemowi, kierownicy programów, technolodzy. Użytkownicy końcowi to osoby korzystające z usług w chmurze jako bezpośredni klienci dostawcy usługi w chmurze, odbiorcy usługi w chmurze korzystającego z usługi w chmurze lub osoby zatrudnione przez odbiorcę usługi w chmurze. Użytkownik jest w ogólnym pojęciu powiązany z dowolnym podmiotem korzystającym z usługi w chmurze. W zależności od scenariusza, użytkownik może być nazywany, w stosownych przypadkach, albo odbiorcą usługi w chmurze, albo użytkownikiem końcowym.

[5] Patrz – rozdział Referencje. Cyfry podane w nawiasach kwadratowych [ ] odnoszą się do pozycji wyszczególnionych w rozdziale Referencje.

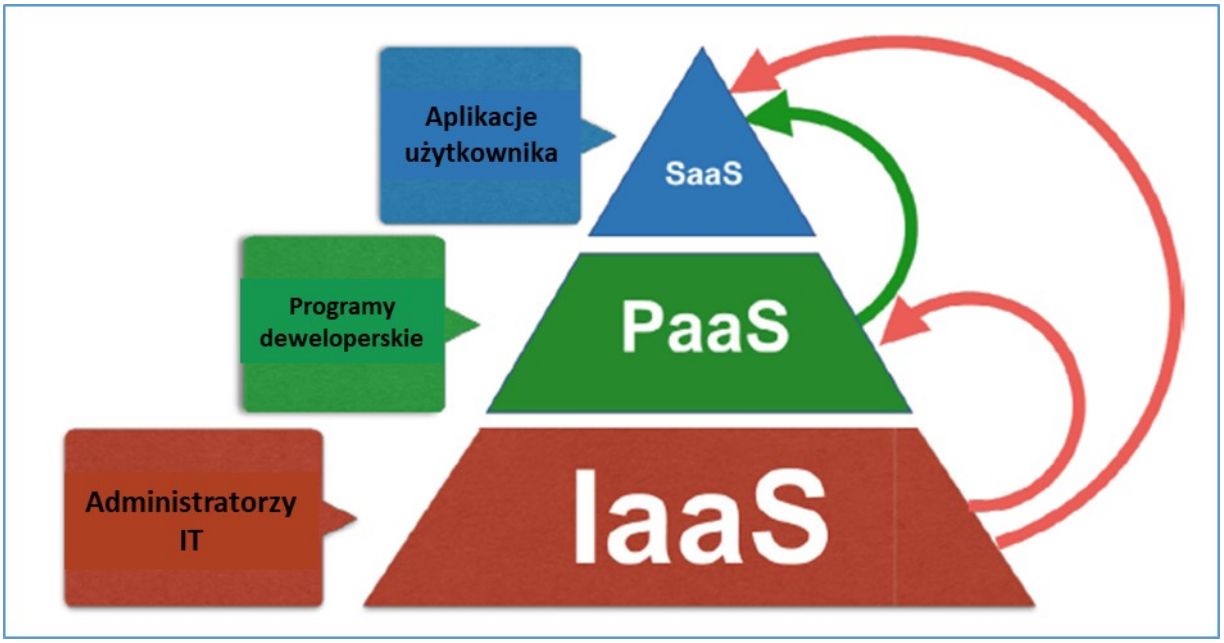
sieciowy na żądanie do wspólnej puli konfigurowalnych zasobów obliczeniowych (np. sieci, serwerów, pamięci masowej, aplikacji i usług), które mogą być szybko dostarczone i uwolnione przy minimalnym wysiłku zarządzania lub interakcji z dostawcą usług [2, 3]. Systemy przetwarzania w chmurze mogą być wdrażane prywatnie, umieszczane w lokalu odbiorcy lub dedykowanej infrastrukturze dostawcy lub publicznie udostępniane przez jednego lub więcej dostawców usług w chmurze. System może być skonfigurowany i użytkowany przez jednego odbiorcę usług chmurowych lub grupę zaufanych partnerów albo obsługiwać wielu klientów, a także może być użytkowany publicznie przez różnych użytkowników końcowych, którzy nabywają usługę. W zależności od rodzaju modelu wdrożenia chmury, chmura może mieć ograniczone prywatne zasoby obliczeniowe lub dostęp do dużych ilości zdalnie dostępnych zasobów. Różne modele wdrożenia przedstawiają szereg kompromisów dotyczących sposobu, w jaki klienci mogą kontrolować swoje zasoby, jak również skalę, koszt i dostępność tych zasobów [4]. Jak przedstawiono na rysunku 1, architektura systemu chmury składa się na ogół z warstw funkcji:

- VM (wirtualna maszyna), w tym:
  - ✓ aplikacje (App),
  - ✓ programowy interfejs aplikacji (API),
  - ✓ system operacyjny (OS).
- Wirtualizator (Hypervisor).
- Pamięci masowe (Storage).
- Sieć wymiany informacji (Networking).
- Sprzęt komputerowy (Hardware).



Rysunek 1. Ogólna architektura systemu chmurowego.

Usługa w chmurze może zapewnić dostęp do aplikacji programowych, takich jak poczta elektroniczna lub narzędzia biurowe (tj. oprogramowanie jako usługa, model usługowy SaaS), środowisko dla klientów do budowania i obsługi własnego oprogramowania (tj. platforma jako usługa, model usługowy PaaS) lub dostęp sieciowy do zwirtualizowanych zasobów obliczeniowych, takich jak moc obliczeniowa i przechowywanie danych (tj. infrastruktura jako usługa, model usługowy IaaS). Każdy z modelu usług chmurowych posiada różne mocne strony i jest odpowiedni dla różnych klientów i celów biznesowych [3], co ilustruje rysunek 2.



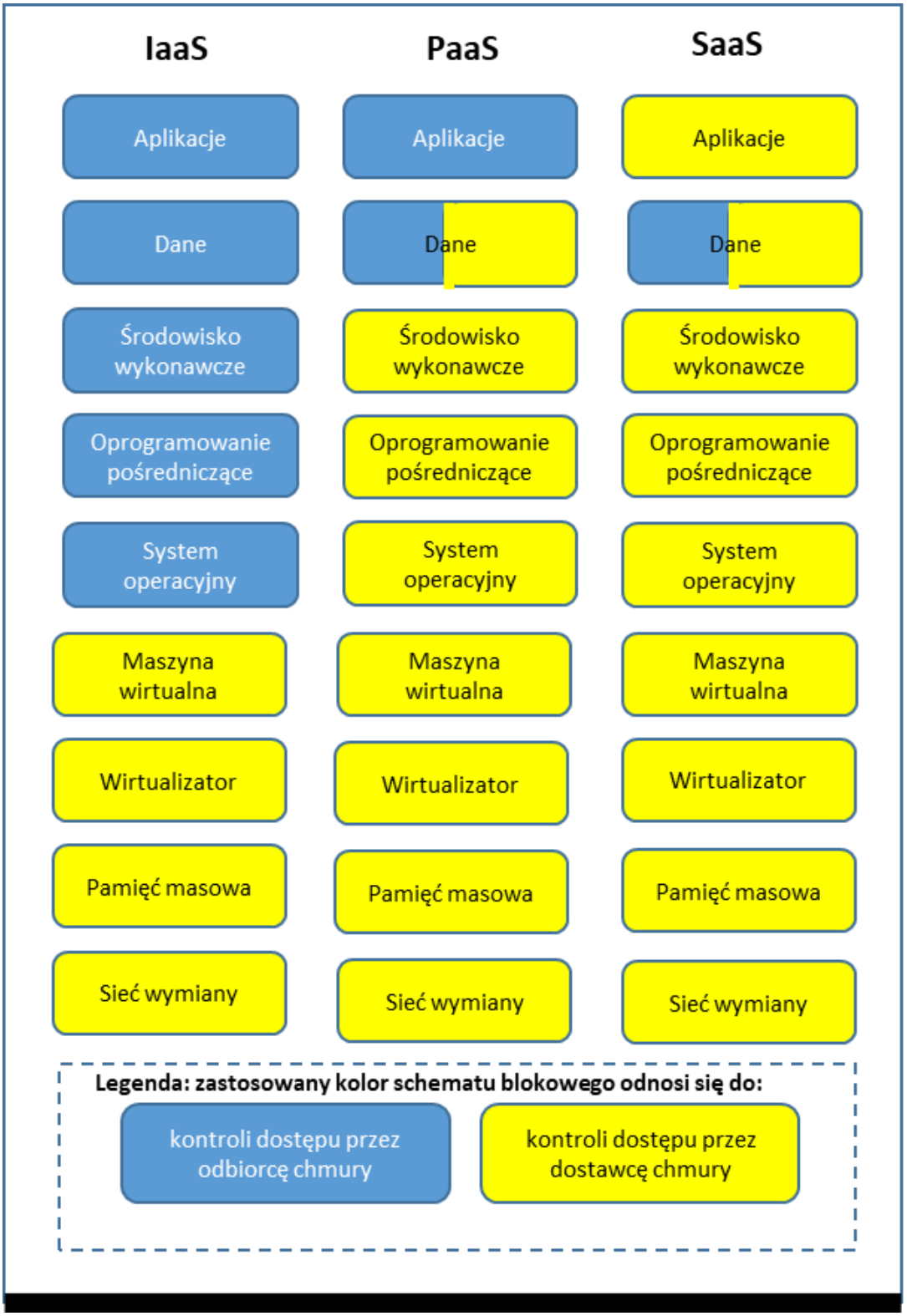
Rysunek 2 Modele usług chmurowych.

System chmury, w którym zastosowano model SaaS, może być dostępny w sieci dla użytkownika końcowego z wykorzystaniem różnych urządzeń klienckich (np. interfejs cienkiego klienta, taki jak przeglądarka internetowa, umożliwiający dostęp do aplikacji poczty elektronicznej) lub poprzez program z odpowiednim zestawem interfejsów, które umożliwiają komunikację z aplikacją chmury. W modelu SaaS użytkownik aplikacji nie zarządza, ani nie kontroluje bazowej infrastruktury chmury, która zazwyczaj obejmuje sieć, serwery, systemy operacyjne, pamięć masową lub poszczególne aplikacje.

Model PaaS w systemie chmury pozwala programistom na tworzenie i wdrażanie aplikacji w infrastrukturze chmury przy użyciu języków programowania, bibliotek, usług i narzędzi. Programista nie zarządza podstawową infrastrukturą chmury ani jej nie kontroluje, ale ma kontrolę nad wdrożonymi aplikacjami (oprogramowaniem) oraz ewentualnie, ustawieniami konfiguracyjnymi dla środowiska hostującego aplikacje.

Usługa IaaS w chmurze zapewnia obliczenia, zwirtualizowaną pamięć masową i zasoby sieciowe dla konsumentów w celu wdrożenia i uruchomienia dowolnego oprogramowania, w tym systemów operacyjnych i aplikacji. Konsumenci mogą mieć kontrolę nad wirtualną pamięcią masową, zwirtualizowanymi komponentami sieciowymi, i możliwością wdrażania własnych maszyn wirtualnych i aplikacji.

Analizując odpowiedzialność odbiorców i dostawców usług w chmurze za ochronę danych w chmurze, nie zawsze jest jasne, czy system IaaS zapewnia tylko zasoby obliczeniowe, czy też oferuje odbiorcom zwirtualizowaną pamięć masową i zasoby sieciowe do wdrażania i uruchamiania dowolnego oprogramowania, w tym systemów operacyjnych i aplikacji. Odbiorca może z kolei mieć kontrolę nad wirtualną pamięcią masową, zwirtualizowanymi komponentami sieciowymi oraz możliwością wdrażania własnych maszyn wirtualnych i aplikacji, które są udostępniane przez dostawcę usług w chmurze. Współodpowiedzialność za kontrolę dostępu musi być rozważana w modelu PaaS i SaaS [42]; Na przykład deweloperzy oprogramowania mogą wymagać dostępu do danych w systemach dostarczanych przez PaaS dla swoich potrzeb rozwojowych, a użytkownicy wewnętrzni aplikacji (tj. użytkownicy, którzy muszą mieć dostęp do danych systemu aplikacji) mogą potrzebować dostępu do danych systemu aplikacji, który jest zarządzany przez aplikacje. Ogólnie rzecz biorąc, w przypadku PaaS, deweloperzy oprogramowania na potrzeby odbiorców mogą dzielić się obowiązkami w zakresie kontroli dostępu z dostawcami usług w chmurze; w przypadku SaaS, wewnętrzni użytkownicy aplikacji mogą dzielić się takimi obowiązkami z dostawcami usług w chmurze. Należy zauważyć, że o ile nie istnieje wyraźna uprzednia zgoda odbiorcy, dostawca PaaS lub SaaS musi zarządzać kontrolą dostępu z dostawcą IaaS i odbiorcą (jeśli nie jest on również dostawcą IaaS). Jeśli odbiorca wyrazi zgodę, dostawca powinien poinformować odbiorcę o zamiarze przechowywania określonych danych u dostawcy IaaS, gdzie będą one dostępne, a także o zakresie, w jakim dane te mogą być dostępne u dostawcy IaaS.



Rysunek 3. **Zarządzanie dostępem przez dostawcę i konsumenta rozwiązań chmurowych.**

Pięć podstawowych cech, które mają wpływ na konstrukcję systemu AC, podsumowano w następujący sposób [2]:

1. Szeroki dostęp do sieci: Usługi w chmurze są dostępne w sieci i udostępniane za pośrednictwem standardowych mechanizmów, które promują korzystanie z heterogenicznych platform grubego i cienkiego klienta (np. telefonów komórkowych, tabletów, laptopów, stacji roboczych). Wywołuje to zagrożenie bezpieczeństwa w związku z dostępem sieciowym. Na przykład, ataki typu „odmowa świadczenia usługi" (*ang. denial of service - DoS*) mogą być przeprowadzane przeciwko systemowi chmurowemu, przez co jego zasoby stają się niedostępne dla prawowitych użytkowników. W związku z tym należy zarządzać AC w odniesieniu do dostępu sieciowego.
2. Buforowanie zasobów: Zasoby obliczeniowe systemu chmury obliczeniowej (np. pamięć masowa, pamięć operacyjna, moc obliczeniowa, przepustowość sieci) są buforowane w celu obsługi wielu odbiorców przy użyciu modelu wielodostępu (*ang. multi-tenant*) poprzez różne zasoby fizyczne i wirtualne, z których każdy jest dynamicznie przydzielany, odłączany i ponownie przydzielany zgodnie z zapotrzebowaniem odbiorców chmury. Informacje mogą wyciec, jeżeli zasoby przydzielone odbiorcy chmury mogą być dostępne dla innego odbiorcy lub jeżeli przydzielone zasoby, takie jak pamięć, nie zostaną wymazane przed ich ponownym przydzieleniem innemu odbiorcy. Istnieje również poczucie niezależności od lokalizacji, polegające na tym, że odbiorca na ogół nie ma kontroli ani wiedzy na temat dokładnej lokalizacji dostarczanych zasobów. Lokalizacja może być określona na wyższym poziomie abstrakcji (np. kraj, państwo, centrum danych), co rodzi obawy o bezpieczeństwo. W związku z tym, w projekcie AC należy uwzględnić metody wdrażania łączenia zasobów przy jednoczesnym zapewnieniu izolacji zasobów wspólnych.
3. Wysoka elastyczność: Usługi w chmurze mogą być dostarczane i uwalniane w sposób elastyczny - automatycznie, w niektórych przypadkach - w sposób zapewniający szybką skalowalność, stosownie do potrzeb. Dla odbiorców chmury zasoby często wydają się być nieograniczone i są przydzielane w dowolnej ilości,

w dowolnym momencie, co dzieje się poprzez dodanie nowych maszyn wirtualnych (VM) o określonych zasobach obliczeniowych. Wyzwaniem dla projektu AC jest zdolność do szybkiej weryfikacji bezpieczeństwa nowych maszyn wirtualnych i określenia, czy nowe dodane maszyny wirtualne kwalifikują się do wykonania określonego zadania.

4. Pomiar usługi: Systemy chmurowe automatycznie kontrolują i optymalizują wykorzystanie zasobów poprzez wykorzystanie możliwości pomiarowych na pewnym poziomie abstrakcji odpowiednim dla typu usługi (np. magazynowanie, przetwarzanie, przepustowość, aktywne konta użytkowników końcowych). Zużycie zasobów jest monitorowane, kontrolowane i raportowane w celu zapewnienia przejrzystości zarówno dla dostawcy, jak i odbiorców korzystających z danej usługi. Aby utrzymać wykorzystanie zasobów, odbiorcy usługi w chmurze powinni mieć upoważnienie do przeglądania, ale nie modyfikowania własnych danych pomiarowych, ponieważ może to prowadzić do sfałszowania płatności wymaganych za usługi w chmurze. Zatem uzasadnione jest, aby AC uwzględniła ochronę danych pomiarowych.

5. Udostępnianie danych: Dzielenie się informacjami między różnymi podmiotami nie jest trywialnym zadaniem, ponieważ system chmury musi spełniać te same wymagania bezpieczeństwa, co systemy podmiotu. W celu ułatwienia wymiany danych, należy rozważyć takie pojęcia jak zaufanie do połączonych tożsamości i atrybutów AC, a następnie zbudować takie zaufanie, które jest kluczowe. W niniejszym dokumencie przyjęto założenie, że zaufanie i tożsamości/atrybuty są już ustanowione, a dalsze omówienie tego tematu zostanie rozważone w innym dokumencie. Niezależnie od modelu usługi, odbiorcy są odpowiedzialni za bezpieczeństwo swoich danych w chmurze i domyślnie za to, kto ma do nich dostęp [5]. Z tego powodu dane nigdy nie są kontrolowane przez dostawców usługi w chmurze, a kontrola w tym zakresie pozostaje w gestii odbiorcy usługi chmurowej. Wyjątek stanowią dane znajdujące się w logach, jednakże należy rozważyć, w jaki sposób takie dane wpływają na prywatność i bezpieczeństwo. Chociaż dostawca usługi w chmurze może stać się administratorem danych

odbiorców chmury, jednak nie powinien on mieć dostępu do tych danych. Jeżeli dane odbiorców nie są zaszyfrowane, wówczas administratorzy chmury mogą mieć możliwość ich odczytania. W takim przypadku dane odbiorcy powinny być zidentyfikowane (poprzez prawa dostępu dostawcy do danych) i oznaczone czerwoną flagą, jako dostępne u dostawcy usług, a odbiorca powinien zostać o tym niezwłocznie poinformowany.

Wytyczne dla każdego modelu usługi w chmurze, opisane w rozdziałach 3, 4 i 6 niniejszego dokumentu, mogą być dalej rozszerzone o wymagania systemowe poprzez odniesienie do elementów kontroli AC wymienionych w publikacji NSC 800-53, *Zasady stosowania zabezpieczeń w systemach informacyjnych podmiotów publicznych [6]* w oparciu o wymagania operacyjne usługi w chmurze. Załącznik A dokumentu NSC 800-210 mapuje wskazówki dotyczące elementów kontroli AC wymienione w NSC 800-53.

3. WYTYCZNE DOTYCZĄCE SYSTEMÓW KONTROLI DOSTĘPU W MODELU IAAS

IaaS jest podstawą wszystkich usług w chmurze, które oferują przetwarzanie i przechowywanie danych poprzez sieć, taką jak Internet. Dzięki technologii wirtualizacji, IaaS umożliwia użytkownikom końcowym dynamiczne przydzielanie zasobów obliczeniowych poprzez uruchamianie nowych maszyn wirtualnych (VM) lub uwalnianie ich zgodnie z potrzebami użytkownika. Maszyna wirtualna to kontener z oprogramowaniem, który zachowuje się jak maszyna fizyczna z własnym systemem operacyjnym (OS) i zasobami wirtualnymi (np. CPU, pamięć, dysk twardy itp.). Wynajem maszyn wirtualnych jest bardziej opłacalny niż zakup nowych maszyn fizycznych. Technologia wirtualizacji składa się z maszyn wirtualnych i wirtualizatora (ang. hypervisor), jak pokazano na rysunku 1. Maszyny wirtualne są zarządzane przez wirtualizator, który kontroluje przepływ danych i instrukcji pomiędzy maszynami wirtualnymi, a sprzętem fizycznym. Po stronie odbiorcy, zazwyczaj administratorzy systemów są głównymi użytkownikami usług IaaS, ponieważ usługi IaaS są elastyczne w konfiguracji zasobów (np. sieci, przechowywania danych).

Wirtualizacja wprowadza dodatkowe obciążenia w zakresie zarządzania bezpieczeństwem poprzez wprowadzenie środków bezpieczeństwa, które wynikają z połączenia wielu maszyn wirtualnych w jeden komputer fizyczny, co może mieć potencjalnie negatywny skutek w przypadku wystąpienia zagrożenia bezpieczeństwa. Niektóre systemy chmury obliczeniowej ułatwiają współdzielenie informacji między maszynami wirtualnymi, na przykład umożliwiając użytkownikom tworzenie wielu maszyn wirtualnych w obrębie tego samego wirtualizatora. Wygoda ta może jednak również stać się wektorem ataku, ponieważ pomiędzy maszynami wirtualnymi może dojść do wycieku danych. Dodatkowo, zwirtualizowane środowiska mają charakter tymczasowy, ponieważ są tworzone i znikają, co komplikuje tworzenie i utrzymywanie niezbędnych granic bezpieczeństwa.

Jak pokazano na rysunku 3, dane w oprogramowaniu pośredniczącym, aplikacjach i warstwach operacyjnych są własnością klienta i są przez niego kontrolowane. System IaaS i klient muszą zapewnić, że dostęp do danych nie jest udzielany administratorom

systemu IaaS, ani żadnym innym klientom IaaS w tych warstwach, chyba, że którykolwiek z nich jest dozwolony. Administratorzy systemu IaaS są odpowiedzialni za kontrolę dostępu do wirtualnej maszyny, wirtualizatora, pamięci masowej i warstw sieciowych i powinni uwzględnić wytyczne zawarte sekcjach 3.1 - 3.5.

3.1. WYTYCZNE DLA SIECI

Sieć jest współdzielona przez klientów IaaS i ważne jest, aby zabezpieczyć ruch sieciowy i środowisko chmury przed wykorzystaniem przez nieautoryzowanych klientów. W związku z tym wymagana jest kontrola dostępu do granic sieci i białych list do komunikacji sieciowej, którą można zastosować poprzez np. dedykowane wirtualne sieci lokalne (*ang. virtual local area network- VLAN*) wykorzystujące automatyczne listy kontroli dostępu (*ang. access control list - ACL*). Użycie tagowania VLAN zgodnego ze standardem 802.1Q 454 Institute of Electrical and Electronics Engineers (IEEE) dla ruchu sieciowego z centrum danych w chmurze spowoduje przekierowanie tylko ruchu oznaczonego numerem z unikatowym identyfikatorem VLAN serwera do lub z tego serwera [7].

3.2. WYTYCZNE DLA WIRTUALIZATORA

Wirtualizator odgrywa ważną rolę w bezpieczeństwie całej zwirtualizowanej architektury, ponieważ zarządza obciążeniami klientów i systemami operacyjnymi gości (OS)[6], tworzy nowe obrazy systemów operacyjnych gości oraz kontroluje zasoby sprzętowe. Implikacje związane z bezpieczeństwem takich działań jak zarządzanie systemami operacyjnymi gości i zasobami sprzętowymi powodują, że dostęp do wirtualizatora powinien być ograniczony tylko dla uprawnionych administratorów chmury. W przeciwnym razie użytkownik końcowy chmury mógłby potencjalnie uzyskać maszynę wirtualną od dostawcy usług w chmurze i zainstalować złośliwy system operacyjny gościa, który naraża wirtualizator na szwank, uzyskując

[6] System operacyjny gościa (*ang. guest OS*) to system operacyjny (OS), który jest zainstalowany na maszynie wirtualnej, w odróżnieniu od systemu operacyjnego zainstalowanego na maszynie fizycznej, zwanego systemem operacyjnym gospodarza (hosta). System operacyjny gościa jest częścią systemu podzielonego na partycje lub częścią maszyny wirtualnej (VM). System operacyjny gościa stanowi alternatywny system operacyjny dla urządzenia.

nieautoryzowany dostęp do innych maszyn wirtualnych i zmieniając ich pamięć [8]. Ponadto atak na maszynę wirtualną o niższych prawach dostępu może być w stanie zwiększyć swoje uprawnienia dostępu do wyższego poziomu, naruszając przydział zasobów sprzętowych w obrębie wirtualizatora [9]. Ochrona wirtualizatora przed nieautoryzowanym dostępem jest zatem krytyczna dla bezpieczeństwa usług IaaS.

3.3. WYTYCZNE DLA MASZYN WIRTUALNYCH

Maszyny wirtualne, które są tworzone przez użytkowników końcowych, pozwalają na współdzielenie tych samych zasobów fizycznych pomiędzy wieloma użytkownikami końcowymi. W takim przypadku należy dopilnować, aby żadna aplikacja z jednej maszyny wirtualnej nie miała bezpośredniego dostępu do innych maszyn wirtualnych, ponieważ ukryte kanały 10, 11] mogą powodować wyciek informacji pomiędzy maszynami wirtualnymi poprzez dostęp do współdzielonych zasobów fizycznych (np. pamięci). Podobnie, możliwość kopiowania i wklejania informacji pomiędzy VM za pośrednictwem schowka jest wygodną funkcją, to jednak taka możliwość mogłaby zostać udostępniona innym VM działającym na tym samym wirtualizatorze i w ten sposób wprowadzić wektor ataku (tzn. informacje mogłyby wyciekać do innych VM za pośrednictwem schowka). Podmioty powinny posiadać zasady dotyczące korzystania ze wspólnych schowków. Izolacja pomiędzy wirtualnymi maszynami jest konieczna, aby utrzymać ich działanie niezależnie od siebie, a limity wykorzystania zasobów wirtualnych powinny być regulowane w taki sposób, aby złośliwa maszyna wirtualna nie mogła doprowadzić do wyczerpujących zasobów obliczeniowych. Jeżeli złośliwa aplikacja zużywa większość zasobów obliczeniowych, legalne aplikacje mogą nie być w stanie uzyskać zasobów wystarczających do wykonania swoich operacji. Co więcej, użytkownicy końcowi mogą przerwać wykonywanie swoich zadań przed ich zakończeniem. Stan i dane obecnej maszyny wirtualnej byłyby wówczas zapisywane jako obraz systemu operacyjnego gości, a po wznowieniu zadania maszyna wirtualna mogłaby zostać przeniesiona do innego wirtualizatora. W takich scenariuszach obrazy systemów operacyjnych gości muszą być chronione przed nieautoryzowanym dostępem, manipulacją lub przechowywaniem. Co więcej, nieaktywne maszyny

wirtualne mogą również przechowywać dane wrażliwe. Powinno być brane pod uwagę monitorowanie dostępu do wrażliwych danych nieaktywnych maszyn wirtualnych.

3.4. WYTYCZNE DLA API

Istnieje kilka popularnych platform open-source do wdrażania chmury IaaS [12, 13, 14]. Platformy te umożliwiają interfejsom API zarządzanie kontrolą dostępu do maszyn wirtualnych, wirtualizatorów i sieci (uwaga – dany odbiorca nie może kontrolować wirtualizatorów i sieci w środowisku z wieloma odbiorcami, chyba, że odbywa się to w chmurze prywatnej). Na przykład, publikacja [14] składa się z komponentów kontroli w odniesieniu do API, komunikacji, cyklu życia, pamięci masowej, woluminu, harmonogramu, sieci, serwera API do zarządzania politykami AC dla wirtualizatorów oraz kontrolera sieci do konstruowania mostów sieciowych i zapory sieciowej AC. Brak monitorowania AC w ramach tych API może skutkować nieegzekwowaniem lub niewłaściwym egzekwowaniem zasad AC przez wirtualizatory, maszyny wirtualne i sieci. W związku z tym należy również wziąć pod uwagę usługę monitorowania AC interfejsów API na platformach chmurowych.

3.5. ZALECENIA DOTYCZĄCE KONTROLI DOSTĘPU DO USŁUG IAAS

Jak pokazano w poprzednich sekcjach, bezpieczeństwo systemu chmury IaaS jest w dużej mierze zależne od wirtualizacji (wirtualizatora). Jednym z najczęściej stosowanych rozwiązań służących ich ochronie jest system zarządzania wirtualizacją [15], który znajduje się pomiędzy sprzętem fizycznym, a wirtualizatorem. System zarządzania wirtualizacją wymusza AC zarówno w wirtualizatorach, jak i w maszynach wirtualnych na różne sposoby. Systemy zarządzania wirtualizacją wymuszają różne poziomy dostępu dla różnych użytkowników. Niektórzy użytkownicy mają dostęp do interfejsu administracyjnego systemu operacyjnego klienta tylko do odczytu, niektórzy mogą kontrolować poszczególne systemy operacyjne klienta, a niektórzy mają pełną kontrolę administracyjną.

Istnieją już rozwiązania w zakresie dostarczania AC dla wirtualizatorów i maszyn wirtualnych. Dla przykładu, podejście w przedstawione w [16] zabezpiecza wirtualizator przed atakami typu „przejęcie kontroli' (*ang. control hijacking*), chroniąc jego kod przed nieautoryzowanym dostępem i oferując izolację maszyn wirtualnych

z elastycznym zabezpieczeniem w postaci obowiązkowej kontroli dostępu (*ang. mandatory access control - MAC*). Aby wyegzekwować AC w zakresie interoperacyjności, można zastosować dobrze zaprojektowane porozumienie o poziomie usług (SLA) w celu zabezpieczenia zewnętrznej interoperacyjności. Inne mechanizmy izolowania [17, 18] są pomocne w zapewnieniu bezpieczeństwa wewnętrznych operacji.
W tabeli 1 wymieniono wytyczne dotyczące polityki AC w modelu IaaS, które uwzględniają główne elementy AC (tj. podmiot, działanie, obiekt). Każdy wiersz wskazuje ewentualną regułę AC, a projektant AC powinien ostatecznie zdecydować, czy dostęp w każdej regule jest dozwolony, czy też odmawia się mu dostępu na podstawie wymogów systemu. Na przykład, jeżeli legalny użytkownik końcowy IaaS wymaga korzystania z usług w chmurze, powinna zostać przyznana akcja logowania w wirtualizatorze dla użytkownika końcowego; w przeciwnym razie powinna zostać ona zablokowana.

Tabela 1. Zasady polityki AC dla usługi na poziomie IaaS.

Podmiot	Działanie	Obiekt	Warunki środowiskowe
Użytkownik końcowy IaaS	Login, Czytaj, Pisz, Utwórz	Wirtualizator	Czas, lokalizacja, poziom wpływu na bezpieczeństwo itp.
Użytkownik końcowy IaaS	Czytaj, Pisz, Utwórz	VM	Czas, lokalizacja, poziom wpływu na bezpieczeństwo itp.
VM	Pisz	Wirtualizator	Czas, lokalizacja, poziom wpływu na bezpieczeństwo itp.
VM	Czytaj, Pisz	Inne VM w obrębie tego samego hostu	Czas, lokalizacja, poziom wpływu na bezpieczeństwo itp.
VM	Czytaj, Pisz, Utwórz	Obrazy OS użytkowników	Czas, lokalizacja, poziom wpływu na bezpieczeństwo itp.

Podmiot	Działanie	Obiekt	Warunki środowiskowe
VM	Czytaj, Pisz	Inne VM z innych hostów, ale w obrębie tego samego dostawcy IaaS	Czas, lokalizacja, poziom wpływu na bezpieczeństwo itp.
VM	Czytaj, Pisz	Inne VM od innych dostawców IaaS	Czas, lokalizacja, poziom wpływu na bezpieczeństwo itp.
Wirtualizator	Czytaj, Pisz, Utwórz	Obrazy OS użytkowników	Czas, lokalizacja, poziom wpływu na bezpieczeństwo itp.
Wirtualizator	Czytaj, Pisz	Zasoby sprzętowe	Czas, lokalizacja, poziom wpływu na bezpieczeństwo itp.
Wirtualizator	Czytaj, Pisz, Utwórz	VM	Czas, lokalizacja, poziom wpływu na bezpieczeństwo itp.

4. WYTYCZNE DOTYCZĄCE SYSTEMÓW KONTROLI DOSTĘPU W MODELU PAAS

PaaS jest platformą, która zapewnia programistom ramy do tworzenia i wdrażania niestandardowych aplikacji. Jak pokazano na rysunku 3, wszelkie aspekty zapewnienia bezpieczeństwa poniżej poziomu danych i począwszy od poziomu uruchomienia powinny być oferowane przez dostawcę PaaS. Głównym celem AC w modelu PaaS jest ochrona danych w czasie rzeczywistym, zarządzana przez oprogramowanie pośredniczące (*ang. middleware*) i OS. Aby chronić swoje dane przed wyciekiem przez ukryty kanał wprowadzony przez niezabezpieczoną pamięć współdzieloną, aplikacje muszą polegać na bezpieczeństwie i prywatności oferowanymi przez dostawcę PaaS. Dlatego też egzekwowanie AC w stosunku do danych podczas pracy w PaaS jest krytyczne dla bezpieczeństwa usług PaaS.
Jak opisano w wytycznych w sekcjach 4.1-4.6 poniżej, administrator systemu PaaS jest odpowiedzialny za kontrolę dostępu do środowiska wykonawczego (*ang. runtime*), oprogramowania pośredniczącego, systemu operacyjnego, maszyny wirtualnej, wirtualizatora, pamięci masowej i warstw sieciowych.

4.1. WYTYCZNE DOTYCZĄCE PAMIĘCI DANYCH

Model PaaS pozwala użytkownikom na wdrażanie zadań w kontrolowanym przez dostawcę oprogramowaniu pośredniczącym i systemie operacyjnym hosta, które mogą być współdzielone z innymi aplikacjami PaaS. W związku z tym PaaS zazwyczaj korzysta z technik opartych na systemie operacyjnym (np. Linux Containers i Docker do izolowania aplikacji) [19]. Istniejące liczne ataki związane z pamięcią mogą jednak zagrozić wrażliwym danym związanym z aplikacjami poprzez włamanie do współdzielonej pamięci operacyjnej w systemie PaaS [20]. Dlatego też należy rozważyć AC dla pamięci operacyjnej, np. AC w stosunku do różnych procesów w pamięci podręcznej procesora [21].

4.2. WYTYCZNE DOTYCZĄCE API

Ponieważ model PaaS pozwala deweloperom na budowanie aplikacji na platformie, API powinien kontrolować zakres aplikacji każdego użytkownika w taki sposób, że dane użytkownika pozostają niedostępne pomiędzy różnymi aplikacjami. Dodatkowo, spakowany API może być obsługiwany jako mikrousługa w PaaS. Scentralizowana architektura nabywania i egzekwowania polityk dostępu regulujących dostęp do wszystkich mikrousług jest wymagana ze względu na samą liczbę tego rodzaju usług potrzebnych do obsługi rzeczywistych transakcji biznesowych (np. przetwarzania zamówień klientów i wysyłki). Ponieważ każda z mikrousług może być wdrażana w innym języku programowania, tworzenie polityk i na ich podstawie decyzji dotyczących dostępu może wymagać użycia serwera autoryzacyjnego [22].

4.3. REKOMENDACJE DOTYCZĄCE KONTROLI DOSTĘPU W MODELU PAAS

Należy ustanowić skuteczną metodę ochrony danych pamięci poprzez tzw. wypłukanie (*ang. flushing*) pamięci podręcznej procesora podczas przełączania kontekstowego. Aby jednak uniknąć znacznego pogorszenia wydajności, należy usuwać tylko bardzo wrażliwe dane z pamięci.

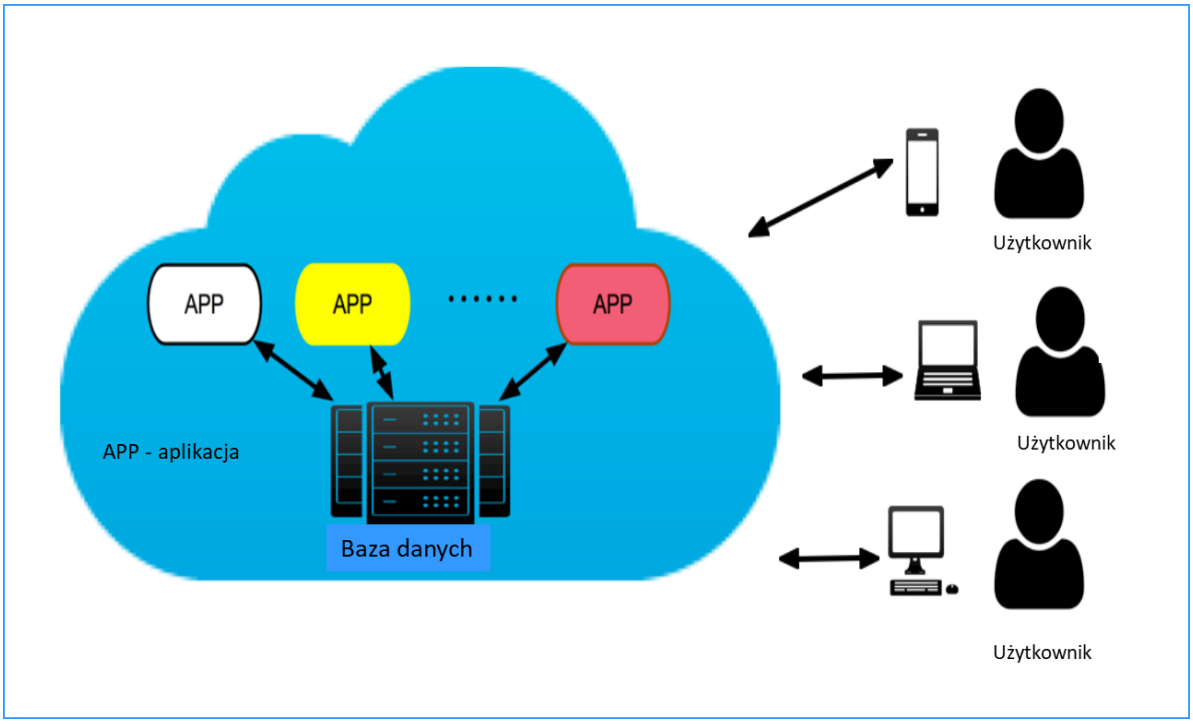
Wytyczne dotyczące polityki AC w modelu PaaS są wymienione w tabeli 2 w odniesieniu do trzech podstawowych elementów AC (tj. podmiot, działanie, obiekt). Każdy wiersz wskazuje ewentualną regułę AC, ale projektant AC powinien zdecydować, czy dostęp powinien zostać przyznany, czy też odrzucony w oparciu o wymogi systemowe. Przykładowo, jeżeli użytkownik aplikacji potrzebuje dostępu do danych pamięci związanych z jego aplikacją, to zostanie mu przyznane pozwolenie na odczyt danych pamięci. Jednakże innym użytkownikom odmówi się dostępu do tych danych.

Tabela 2. Zasady polityki AC dla usługi dla modelu PaaS.

Podmiot	Działanie	Obiekt	Warunki środowiskowe
Użytkownik aplikacji	Czytaj	Pamięć danych	Czas, lokalizacja, poziom wpływu na bezpieczeństwo itp.
VM hostowanej aplikacji	Czytaj, Pisz	Inne aplikacje wewnątrz danego hosta	Czas, lokalizacja, poziom wpływu na bezpieczeństwo itp.
Deweloper aplikacji	Utwórz, Czytaj, Pisz	Dane oprogramowania pośredniczącego, pamięć danych	Czas, lokalizacja, poziom wpływu na bezpieczeństwo itp.
Dostawca chmury	Replikuj	Dane związane z aplikacjami	Czas, lokalizacja, poziom wpływu na bezpieczeństwo itp.

5. WYTYCZNE DOTYCZĄCE SYSTEMÓW KONTROLI DOSTĘPU W MODELU SAAS

W SaaS dostawca usług w chmurze dostarcza użytkownikom końcowym aplikację jako usługę za pośrednictwem sieci takiej jak np. Internet. Nie ma więc potrzeby, aby użytkownicy instalowali i wykonywali aplikacje lokalnie na swoich własnych komputerach. Jak pokazano na rysunku 4, wiele aplikacji i wielu użytkowników może być jednocześnie obsługiwanych przez chmurę, korzystając ze współdzielonych zasobów, w tym aplikacji i baz danych.



Rysunek 4. Architektura wielodostępu w modelu SaaS.

Jeśli deweloper używa aplikacji innej firmy, dane mogą być przechowywane w tej aplikacji oraz w innych aplikacjach niepowiązanych. Użytkownicy końcowi, aby chronić swoje dane przed nieautoryzowanym dostępem z innych aplikacji, muszą polegać na bezpieczeństwie i prywatności oferowanej przez dostawcę usługi w chmurze. Należy pamiętać, że dane zarządzane przez warstwę aplikacji, są własnością i są kontrolowane przez odbiorcę chmury. System SaaS i odbiorca muszą zapewnić, że dostęp do danych aplikacji w tych warstwach nie jest udzielany administratorowi systemu SaaS, innym odbiorcom chmury lub użytkownikom, chyba, że są oni zaufani. Administratorzy

systemu SaaS są odpowiedzialni za kontrolę dostępu do wszystkich warstw operacyjnych pokazanych na rysunku 3 i powinni uwzględnić wytyczne zawarte w rozdziałach 3, 4 oraz sekcjach 5.1- 5.4.

5.1. WYTYCZNE DOTYCZĄCE KONTROLI PRZEZ WŁAŚCICIELA DANYCH

Podmiot korzystający z usług w modelu SaaS jest właścicielem danych znajdujących się w używanych aplikacjach. Dane dotyczące aplikacji są zazwyczaj przechowywane w bazie danych dostawcy usług SaaS. To, jak dostawca danych zarządza dostępem do swoich danych jest wyzwaniem. Przykładowe pytania, na które musi sobie odpowiedzieć dotyczą tego, gdzie i jak długo jego dane są przechowywane przez dostawcę usługi oraz tego, czy dostawca posiada uprawnienia do określania praw dostępu do danych, które przechowuje. Jeśli dostawca danych ma zdolność do określenia praw dostępu do danych, które przechowuje, należy rozważyć, czy w ramach modelu SaaS zawsze przestrzegana jest aktualna polityka AC.

5.2. WYTYCZNE DOTYCZĄCE POUFNOŚCI

W modelu SaaS musi być chroniona integralność danych wrażliwych znajdujących się w domenie właściciela danych. Mechanizmy ochrony danych aplikacji obejmują systemy szyfrowania danych za pomocą kluczy szyfrujących, które będą ujawniane tylko upoważnionym użytkownikom [23]. Mechanizmy do zarządzania, szyfrowania i odszyfrowywania danych dotyczących aplikacji powinny ustalać tożsamość użytkowników z wykorzystaniem systemy kontroli dostępu opartego na atrybutach (*ang. attribute-based access control -ABAC*) [24] i szyfrowaniu opartym na atrybutach (*ang. attribute-based encryption - ABE*) [23, 25, 26, 27, 28]. Biorąc jednak pod uwagę dużą ilość danych w modelu SaaS, związane z tym szyfrowanie i odszyfrowywanie znacznie zmniejszają wydajność systemu. W związku z tym, przy szyfrowaniu należy zwrócić uwagę na zapewnienie odpowiedniego poziomu poufności danych przy jednoczesnym zapewnieniu dobrej wydajności.

5.3. WYTYCZNE W ZAKRESIE ZARZĄDZANIA PRZYWILEJAMI

Oprócz egzekwowania AC, zarządzanie uprawnieniami obejmuje dodanie, usunięcie i zmianę uprawnień danej osoby lub procesu. Istotne jest zaprojektowanie elastycznego

mechanizmu nadawania i odbierania uprawnień w celu utrzymania użyteczności usługi SaaS [29].

5.4. WYTYCZNE DOTYCZĄCE WIELOKROTNEJ REPLIKACJI DANYCH

W celu utrzymania wysokiej dostępności usługi, dostawca usługi w chmurze może replikować dane w wielu miejscach, nawet w różnych krajach. Dlatego ważne jest, aby upewnić się, że wszystkie repliki danych są chronione na podstawie tej samej polityki AC. Innymi słowy, ta sama polityka AC dla replikowanych danych powinna być dostępna dla wszystkich hostów, które przetwarzają te same dane. Musi być również brana pod uwagę technologia synchronizacji polityki po jej zmianach.

5.5. WYTYCZNE DOTYCZĄCE WIELODOSTĘPU (*ANG. MULTI-TENANCY*)

Model SaaS wprowadza dodatkowe aspekty w odniesieniu do zarządzania dostępem do aplikacji. Pilną koniecznością jest skupienie się na dostępie użytkowników do aplikacji. Prawa dostępu są przyznawane użytkownikom końcowym za pośrednictwem polityk AC w oparciu o predefiniowane atrybuty lub role. Wymogi w tym zakresie mogą zostać określone za pomocą modeli polityki kontroli dostępu opartych na atrybutach (ABAC) [30, 31], kontroli dostępu opartej na rolach (*ang. role-based access control - RBAC*) [32] oraz kontroli dostępu opartej na kontekście (*ang. context-based access control - CBAC*) [33].

Użytkownik korzysta z aplikacji jako z usługi. Model SaaS jest typową platformą wielodostępową, która obsługuje wielu użytkowników końcowych mających jednoczesny dostęp do aplikacji oraz danych różnych aplikacji znajdujących się w tej samej lokalizacji. Wykorzystanie podatności w aplikacji lub wstrzyknięcie kodu klienta do systemu SaaS może narazić dane innych użytkowników [34]. W związku z tym, przy projektowaniu systemu AC należy zwrócić uwagę na to, aby zachodziła separacja danych w aplikacjach różnych użytkowników.

5.6. WYTYCZNE W ZAKRESIE ZARZĄDZANIA POPRZEZ ATRYBUTY I ROLE

W modelu usług SaaS, zarządzanie AC oparte na atrybutach i rolach wykorzystuje polityki i predefiniowane role do zarządzania prawami dostępu do aplikacji i baz danych. Podstawowym wyzwaniem związanym z wdrożeniem zarządzania AC

opartego na atrybutach lub rolach jest osiągnięcie porozumienia co do tego, jakie powinny być stosowane atrybuty lub role i co powinno być brane pod uwagę przy projektowaniu systemów AC [35]. Jeśli zestaw rozpatrywanych atrybutów lub ról jest zbyt mały, elastyczność takiego systemu zostanie ograniczona. Jeżeli jednak liczba atrybutów lub ról jest zbyt duża wzrośnie złożoność polityk.

5.7. WYTYCZNE W ZAKRESIE STOSOWANYCH POLITYK

Aplikacje SaaS zapewniają specyficzne dla danej aplikacji konfiguracje kontroli dostępu dla różnych aplikacji użytkownika, a w tym przypadku polityki użytkownika dla każdej aplikacji są egzekwowane przez dostawcę SaaS. Taka konfiguracja nie obsługuje współpracy między dostawcą SaaS, a infrastrukturą kontroli dostępu użytkownika (odbiorcy). Na przykład, podczas gdy duże organizacje często stosują w lokalach systemy kontroli dostępu do centralnego i efektywnego zarządzania użytkownikami, aplikacje SaaS zazwyczaj zapewniają organizacjom interfejs konfiguracji AC do zarządzania politykami AC, co wymusza przechowywanie i ocenę polityk AC po stronie dostawcy SaaS. Takie podejście może skutkować ujawnieniem dostawcy SaaS poufnych danych niezbędnych do oceny polityk AC. W związku z tym należy rozważyć metody egzekwowania zezwoleń od dostawcy SaaS przy jednoczesnym nieujawnianiu dostawcy SaaS szczególnie chronionych danych dotyczących kontroli dostępu. Autoryzacja przedstawiona w publikacji [36] jest skuteczną techniką, która wykorzystuje warstwę pośredniczącą do przekazywania zarządzania politykami kontroli dostępu od dostawcy SaaS do strony użytkownika i egzekwowania polityk w aplikacjach SaaS bez ujawniania wrażliwych danych wymaganych do oceny polityk.

5.8. WYTYCZNE DOTYCZĄCE API

API w modelu SaaS służy jako interfejs pomiędzy serwerem chmury, a jego użytkownikami. API powinien być zaprojektowane tak, aby chronić zarówno przed przypadkowymi jak i złośliwymi próbami obejścia dowolnej polityki AC. Aplikacje dla podmiotu i osób trzecich często opierają się na API, w którym AC ma charakter warstwowy. Na przykład, jeżeli interfejsy API nie wymagają do wykonywania swoich zadań dostępu do pamięci, wówczas polityka AC dotycząca interfejsów API powinna egzekwować zakaz dostępu do pamięci. Dodatkowo, polityka AC powinna być

określona w celu zarządzania procesem autoryzacji dla interfejsów Web API. Na przykład, gdy interfejsy API łączą się za pomocą protokołów SOAP i REST, AC powinien kontrolować, czy umożliwiają użytkownikom końcowym łączenie się z narzędziami i technologiami firmy Microsoft lub innymi niż Microsoft. W przypadku autoryzowanych połączeń API za pośrednictwem protokołów SOAP i REST, kontrola dostępu (AC) powinna zapewnić wszystkie wymagania związane z tym dostępem, przez te protokoły. W przypadku nieautoryzowanych połączeń API za pośrednictwem tych protokołów, AC nie powinna udzielać dostępu lub powinna udzielać dostępu częściowego.

5.9. REKOMENDACJE W ZAKRESIE KONTROLI DOSTĘPU W MODELU SAAS

W odniesieniu do wielodostępu, autoryzacja może być egzekwowana za pomocą systemu scentralizowanego, zdecentralizowanego lub hybrydowego. W scentralizowanym systemie autoryzacji dostawca SaaS zarządza centralną bazą danych autoryzacji dla każdego użytkownika końcowego i jego kont [37]. W zdecentralizowanym lub hybrydowym systemie autoryzacji poszczególni najemcy są odpowiedzialni za całość lub część procesu autoryzacji. Należy pamiętać, że różni najemcy mogą wymagać różnych systemów. Uwzględnienie atrybutów lub ról najemców jest kluczowe przy wyborze najbardziej odpowiedniego systemu. Istnieje wiele sposobów na określenie atrybutów lub ról, np. w modelach ABAC i RBAC [31,32]. Atrybuty lub role muszą być dobrze zaprojektowane i uwzględniać relacje hierarchiczne podczas wdrażania polityk AC dla różnych najemców.
Federacja autoryzacji przedstawiona w publikacji [36] jest skutecznym sposobem egzekwowania zasad AC u dostawcy SaaS. Ogólna architektura oprogramowania pośredniczącego, która uwzględnia wymogi kontroli dostępu stawiane przez najemców i obsługuje lokalne i zdalne atrybuty lub role, może zostać wykorzystana do rozszerzenia i przeniesienia zarządzania polityką AC z dostawcy SaaS na stronę odbiorcy chmury. Takie podejście centralizuje zarządzanie polityką w zakresie kontroli dostępu odbiorców i zmniejsza wymagania w zakresie zaufania wobec dostawcy SaaS. Ponadto należy również określić AC dla operacji wspierających maszyny wirtualne (np. użytkownik końcowy może stworzyć maszynę wirtualną uruchamiającą różne

aplikacje). W ramach wirtualnej maszyny tego samego hosta jedna aplikacja może potrzebować dostępu do kodu aplikacji innych aplikacji, aby zrealizować swoje zadanie. W przeciwieństwie do architektury PaaS, gdzie użytkownik może w pełni zarządzać projektowaniem, testowaniem i rozwojem oprogramowania, użytkownicy SaaS mają ograniczoną kontrolę nad aplikacjami umieszczonymi w serwerach chmury.
W celu uzyskania kontroli przez właściciela nad danymi aplikacji, może być używana umowa dotycząca klasy bezpieczeństwa (*ang. securit class agreement – SCA*) [28]. SCA jest wzajemnie uzgadniana zarówno przez najemcę usługi SaaS, jak i dostawcę tej usługi i jest wykorzystywana do określania przynależności odbiorcy chmury do określonej klasy bezpieczeństwa. Wielokrotne repliki tych samych danych mają ten sam poziom bezpieczeństwa co dostawca dostarczający dane. Oznacza to, że dane pochodzące od konkretnego dostawcy powinny mieć identyczną klasę bezpieczeństwa dla wszystkich replik danych. W rezultacie, w ramach usługi SaaS, hosta kwalifikującego się do realizacji żądania dostępu można określić poprzez odwołanie się do SCA. Dostawca danych może zarządzać dostępem do swoich danych poprzez określenie klas bezpieczeństwa w celu zapewnienia synchronizacji dostawcy danych i hosta usługi w chmurze, określając prawo dostępu do danych. Na przykład, w modelu Bell-LaPadula [38], zakładając, że raport dotyczący pacjenta jest napisany przez lekarza z poświadczeniem poufności, raport może być odczytany tylko przez hosty z takim samym lub wyższym poświadczeniem bezpieczeństwa. Dodatkowo, w przypadku dostępu do wielu źródeł danych, które nie są przeznaczone do uzyskania dostępu w tym samym systemie chmury, nie powinno dochodzić do przecieku danych ze względu na różne klasy bezpieczeństwa tych źródeł danych w SCA w tych różnych systemach chmury. Jednakże ze względu na dużą złożoność obliczeniową szyfrowania i odszyfrowywania, systemy kryptograficzne powinny być starannie zaprojektowane w celu utrzymania wydajności systemów w chmurze przy jednoczesnej ochronie poufności danych.
Infrastruktura zarządzania uprawnieniami (*ang. privilege management infrastructure – PMI*) [39] może być wykorzystana do dynamicznego zarządzania nadawaniem i odbieraniem uprawnień poprzez wykorzystanie atrybutów lub certyfikatów specyfikacji ról w modelu SaaS. PMI określa uprawnienia dla różnych użytkowników

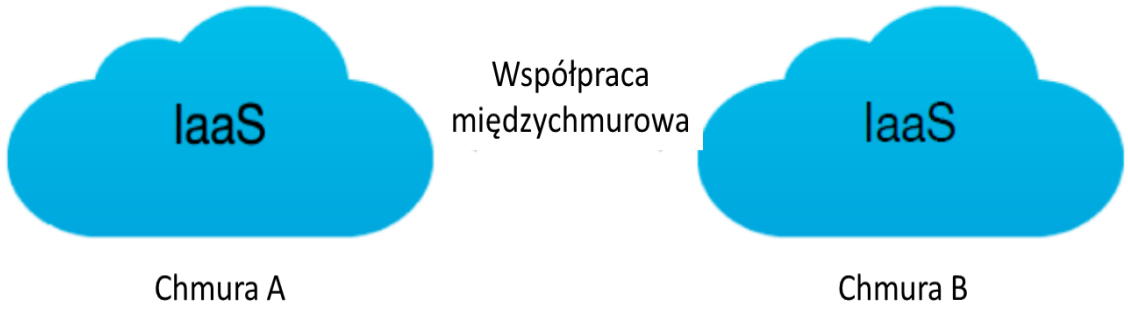
i łączy je z różnymi certyfikatami specyfikacji atrybutów lub ról, które zawierają różne przypisania atrybutów lub ról celu egzekwowania zarządzania tymi uprawnieniami.
W celu obsługi kontroli dostępu do wielu replik danych należy wprowadzić metodę centralnego zarządzania systemem AC. W związku z tym, że dane w ramach dostawcy SaaS są powielane, każda zmiana polityki powinna skutkować odpowiednią aktualizacją centralnej polityki AC. Ponadto polityka AC związana z powielanymi danymi u innych dostawców SaaS powinna być odpowiednio zsynchronizowana w oparciu o politykę AC w systemie centralnym.
Wytyczne AC dotyczące polityki SaaS wymienione są w tabeli 3. Projektant AC powinien zdecydować, czy dostęp w każdej regule jest dozwolony, czy też odmówiony na podstawie wymagań systemowych. Na przykład podczas operacji w federacji chmur dozwolony jest odczyt/zapis maszyny wirtualnej do kodu innej aplikacji w obrębie tego samego hosta, w przeciwnym razie jest on odrzucany.

Tabela 3. Zasady polityki AC dla usługi na poziomie SaaS.

Podmiot	Działanie	Obiekt	Warunki środowiskowe
Użytkownik aplikacji	Czytaj, Pisz	Dane związane z aplikacją	Czas, lokalizacja, poziom wpływu na bezpieczeństwo itp.
Użytkownik aplikacji	Czytaj	Pamięć	Czas, lokalizacja, poziom wpływu na bezpieczeństwo itp.
Użytkownik aplikacji	Wykonaj	Aplikacja	Czas, lokalizacja, poziom wpływu na bezpieczeństwo itp.
Użytkownik aplikacji	Czytaj, Pisz	Dane aplikacji	Czas, lokalizacja, poziom wpływu na bezpieczeństwo itp.
Użytkownik aplikacji	Wykonaj	Kod aplikacji	Czas, lokalizacja, poziom wpływu na bezpieczeństwo itp.
VM hostowanej aplikacji	Wykonaj	Inny kod aplikacji na tym samym hoście	Czas, lokalizacja, poziom wpływu na bezpieczeństwo itp.

6. WYTYCZNE DOTYCZĄCE OPERACJI NA ZEWNĄTRZ I WEWNĄTRZ CHMURY

Ogólnie rzecz biorąc, współpraca (tj. sytuacja, gdy dwa lub więcej systemów działa łącznie) w kontekście chmury może prowadzić do płynnej wymiany danych i usług pomiędzy różnymi infrastrukturami chmury. Istnieją dwa rodzaje współpracy: międzychmurowa i wewnątrzchmurowa. Współpraca międzychmurowa odnosi się do możliwości korzystania z wielu infrastruktur chmury obliczeniowej. Na przykład, jak pokazano na rysunku 5, odbiorca chmury może nabyć usługi IaaS od dwóch różnych dostawców usług w chmurze, chmury A i chmury B, a współpraca między nimi powinna być dozwolona ze uwzględnieniem wymogów dotyczących przetwarzania danych.



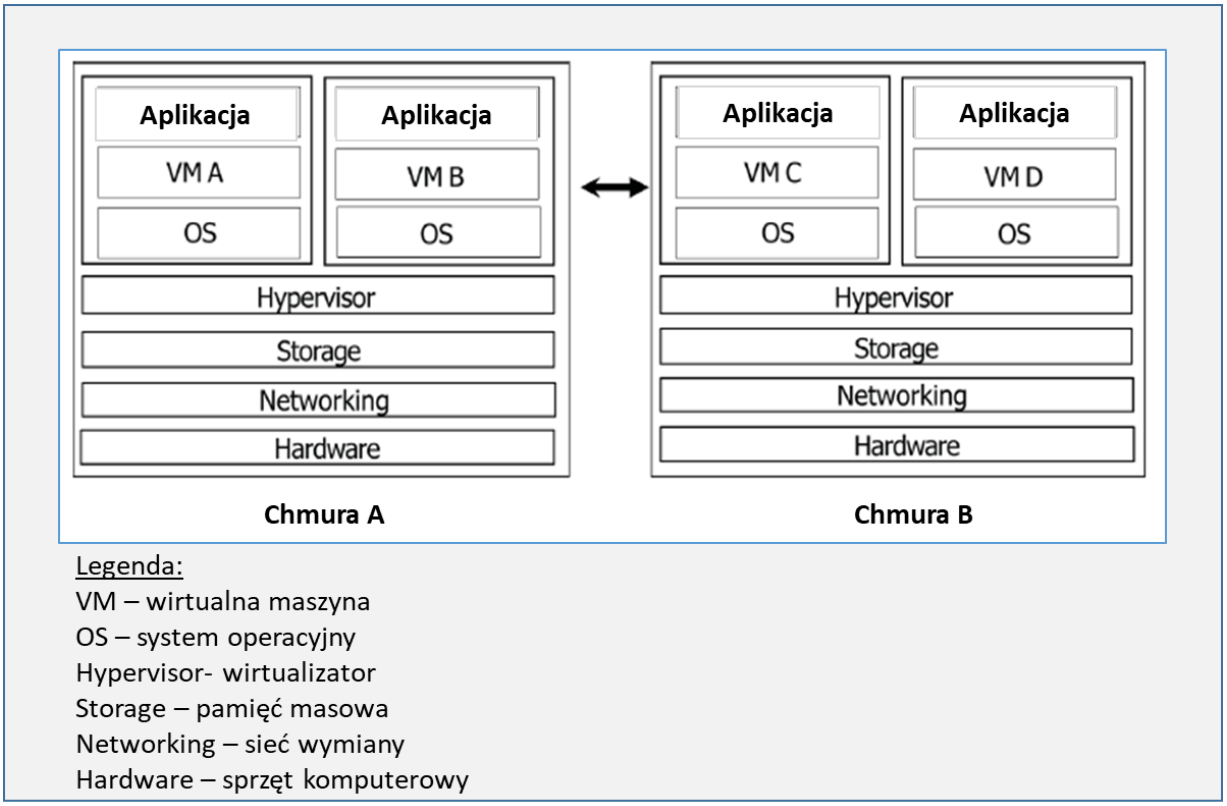
Rysunek 5. Współpraca zewnętrzna (międzychmurowa) pomiędzy różnymi chmurami.

Operacje wewnątrzchmurowe

W przypadku współpracy wewnątrzchmurowej należy rozważyć dwa scenariusze, jak pokazano na rysunku 6. Po pierwsze, odbiorca może posiadać wiele wirtualnych maszyn VM w jednym hostie w chmurze (np. VM A i VM B) i jednocześnie może być wymagana współpraca między tymi maszynami. Po drugie, klient może wynająć wiele hostów w ramach tej samej usługi IaaS i może być wymagana współpraca między tymi różnymi hostami (np. interoperacyjność między VM B i VM C).

W odniesieniu do współpracy wewnątrzchmurowej, polityka AC powinna umożliwiać, podczas okresu współpracy, funkcjonowanie maszyn wirtualnych na potrzeby tego samego odbiorcy, zezwalając na dostęp do każdej z nich oraz wyłączać dostęp po

zakończeniu okresu współpracy. Istnieją dwa podstawowe przypadki w ramach współpracy wewnątrzchmurowej: między hostami (tj. wirtualne maszyny VM pochodzące z różnych hostów chmury współpracują ze sobą) oraz wewnątrz hosta (tj. wirtualne maszyny VM pochodzą z tego samego hosta chmury i muszą wymieniać się danymi i usługami). Ponadto, w przypadku niektórych zastosowań, maszyny wirtualne mogą być rozproszone w wielu komputerach-hostach, a zatem zasady AC powinny obejmować zarówno przypadki wewnątrz-hostowe, jak i międzyhostowe.



Rysunek 6. Wewnątrzchmurowa współpraca w ramach tej samej chmury.

Istnieją pewne kwestie związane z integracją polityki kontroli dostępu w zakresie wzajemnej współpracy. Na przykład różni dostawcy usług w chmurze wykorzystujący różne zestawy atrybutów tematycznych dla AC mogą powodować potencjalne konflikty lub wycieki uprawnień dostępu [40]. Atrybuty o tej samej nazwie mogą skutkować różnymi przywilejami przy zmianie dostawcy. Wyzwaniem jest egzekwowanie AC u różnych dostawców usług w chmurze bez powodowania konfliktów lub blokowania uprawnień dla poszczególnych użytkowników wirtualnych. Wymagałoby to zbadania, w jaki sposób można osiągnąć bezpieczną współpracę

między dostawcami usług w chmurze [1]. Niektóre systemy AC w chmurze przyjmują scentralizowane mechanizmy w celu stworzenia globalnej polityki AC, która zarządza integracją polityki między różnymi dostawcami usług w chmurze [41]. Współpraca między dostawcami usług w chmurze ma jednak charakter przejściowy i w związku z tym jest nieefektywna w zarządzaniu globalną polityką AC, ponieważ poszczególne polityki AC w chmurze są często aktualizowane.

Operacje międzychmurowe

Istnieje możliwość, że niespójne zarządzanie elementami dostępu prowadzi do nieprawidłowej integracji polityki kontroli dostępu w zakresie współpracy międzychmurowej. Na przykład różni dostawcy usług w chmurze wykorzystujący różne zestawy atrybutów tematycznych dla AC mogą powodować potencjalne konflikty lub wycieki uprawnień dostępu [40]. Atrybuty o tej samej nazwie mogą skutkować różnymi przywilejami przy zmianie dostawcy. Egzekwowanie AC wśród różnych dostawców usług w chmurze bez powodowania konfliktów lub blokowania uprawnień dla poszczególnych użytkowników / maszyn wirtualnych jest utrudnione. Wymagałoby to zbadania, w jaki sposób osiągnąć bezpieczną współpracę między dostawcami usług w chmurze [1], np. w środowiskach hybrydowych. Niektóre systemy AC w chmurze przyjmują scentralizowane mechanizmy tworzenia globalnej polityki AC, które zarządzają integracją polityki wśród różnych dostawców usług w chmurze [41]. Jednakże współpraca między dostawcami usług w chmurze ma charakter przejściowy i w związku z tym jest nieefektywna w zarządzaniu globalnymi politykami AC, ponieważ poszczególne polityki AC w chmurze są często aktualizowane.

7. PODSUMOWANIE

Niniejszy dokument stanowi pierwszy krok w kierunku zrozumienia wyzwań związanych z bezpieczeństwem w systemach chmurowych poprzez analizę kwestii kontroli dostępu (AC) we wszystkich trzech modelach dostarczania usług w chmurze - IaaS, PaaS i SaaS. Podsumowano również podstawowe cechy, które miałyby wpływ na konstrukcję AC w chmurze, takie jak szeroki dostęp do sieci, łączenie zasobów, duża elastyczność, mierzalność usług i udostępnianie danych. Proponuje się różne wytyczne dotyczące projektowania AC dla IaaS, PaaS i SaaS, w zależności od ich różnych cech. Uwzględniono również zalecenia dotyczące projektowania AC w różnych systemach chmury w celu ułatwienia przyszłych wdrożeń. Dodatkowo, potencjalne zasady polityki są podsumowane dla każdego systemu chmury. Jednak wiele kwestii pozostaje otwartych, takich jak zarządzanie AC w różnych urządzeniach i platformach, a także nowe wyzwania, które nie pojawiły się jeszcze wraz z powszechnym wdrożeniem chmury.

REFERENCJE

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA[7]	
NSC 199	Standardy kategoryzacji bezpieczeństwa – na podstawie FIPS 199
NSC 200	Minimalne wymagania bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych – na podstawie FIPS 200
NSC 500-292	Architektura referencyjna chmury obliczeniowej - rekomendacje
NSC 800-18	Przewodnik do opracowywania planów bezpieczeństwa systemów informacyjnych w podmiotach publicznych – na podstawie NIST SP 800-18
NSC 800-30	Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne – na podstawie NIST SP 800-30
NSC 800-34	Poradnik planowania awaryjnego – na podstawie NIST SP 800-34
NSC 800-37	Ramy zarządzania ryzykiem w organizacjach i systemach informacyjnych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu – na podstawie NIST SP 800-37
NSC 800-39	Zarządzanie ryzykiem bezpieczeństwa informacji. Przegląd struktury organizacyjnej, misji i systemu informacyjnego – na podstawie NIST SP 800-39
NSC 800-53	Zabezpieczenia i ochrona prywatności systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53

[7] Narodowe Standardy Cyberbezpieczeństwa

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA[7]	
NSC 800-53A	Ocenianie środków bezpieczeństwa i ochrony prywatności systemów informacyjnych oraz organizacji. Tworzenie skutecznych planów oceny – na podstawie NIST SP 800-53A
NSC 800-53B	Zabezpieczenia bazowe systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53B
NSC 800-53 MAP	Mapowanie środków bezpieczeństwa: NSC 800-53 wer. 2 – PN-ISO/IEC 27001:2013; PN-ISO/IEC 27001:2013 – NSC 800-53 wer. 2 Patrz: SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)
NSC 800-60	Wytyczne w zakresie określania kategorii bezpieczeństwa informacji I kategorii bezpieczeństwa systemu informacyjnego – na podstawie NIST SP 800-60
NSC 800-61	Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego – na podstawie NIST SP 800-61

PUBLIKACJE ANGLOJĘZYCZNE[8]	
[1]	Gouglidis A, Mavridis I, Hu VC (2014) Security policy verification for multi-domains in Cloud systems. *International Journal of Information Security* 13(2):97-111. https://doi.org/10.1007/s10207-013-0205-x
[2]	Mell PM, Grance T (2011) The NIST Definition of Cloud Computing. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-145. https://doi.org/10.6028/NIST.SP.800-145
[3]	Liu F, Tong J, Mao J, Bohn R, Messina J, Badger ML, Leaf D (2011), NIST Cloud Computing Reference Architecture. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 500-292. https://doi.org/10.6028/NIST.SP.500-292
[4]	Badger ML, Grance T, Patt-Corner R, Voas JM (2012) Cloud Computing Synopsis and Recommendations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-146. https://doi.org/10.6028/NIST.SP.800-146.
[5]	Federal Information Security Modernization Act of 2014, Pub. L. 113-283, 128 Stat. 3073. https://www.govinfo.gov/app/details/PLAW-113publ283

[8] Publikacje anglojęzyczne zostały podane w celach uzupełniających dla osób zainteresowanych.

PUBLIKACJE ANGLOJĘZYCZNE[8]

[6] Joint Task Force Transformation Initiative (2013) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 4, Includes updates as of January 22, 2015. https://doi.org/10.6028/NIST.SP.800-53r4

[7] Bartock MJ, Souppaya MP, Scarfone KA, Carroll D, Masten R, Scinta G, Massis P, Prafullchandra H, Malnar J, Singh H, Yeluri R, Shea T, Dalton M, Dukes A, Phoenix C. Swarts B (2018) Trust Cloud: Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments. (National Institute of Standards and Technology, Gaithersburg, MD), Preliminary Draft NIST Special Publication (SP) 1800- 19B. Available at https://www.nccoe.nist.gov/projects/building-blocks/trusted-cloud

[8] Szefer J, Lee RB (2011) A case for hardware protection of guest VMs from compromised hypervisors in cloud computing. *2011 31st International Conference on Distributed Computing Systems Workshops (ICDCSW)* (IEEE, Minneapolis, MN), pp 248-252. https://doi.org/10.1109/ICDCSW.2011.51

[9] Krutz RL, Vines RD (2010) *Cloud security: A comprehensive guide to secure cloud computing* (Wiley Publishing, Indianapolis, IN).

[10] Wu J, Ding L, Wu Y, Min-Allah N, Khan SU, Wang Y (2014) C2detector: a covert channel detection framework in cloud computing. *Security and Communication Networks* 7(3):544-557. https://doi.org/10.1002/sec.754

[11] Rushby J (1992) Noninterference, transitivity, and channel-control security policies. (SRI International, Menlo Park, CA), Technical Report CSL-92-02. Available at http://www.csl.sri.com/papers/csl-92-2/

PUBLIKACJE ANGLOJĘZYCZNE[8]

[12] Change ATC, Foster JL, Hall DK (1987) Nimbus-7 SMMR derived global snow cover parameters. *Annals of Glaciology* 9:39-44. https://doi.org/10.3189/S0260305500200736

[13] Nurmi D, Wolski R, Grzegorczyk C, Obertelli G, Soman S, Youseff L, Zagorodnov D (2009) The Eucalyptus open-source cloud-computing system. *9th IEEE/ACM International Symposium on Cluster Computing and the Grid (CCGRID'09)* (IEEE, Shanghai, China), pp 124-131. https://doi.org/10.1109/CCGRID.2009.93

[14] Sefraoui O, Aissaoui M, Eleuldj M (2012) OpenStack: toward an open-source solution for cloud computing. *International Journal of Computer Applications* 55(3):38-42. https://doi.org/10.5120/8738-2991

[15] Scarfone KA, Souppaya MP, Hoffman P (2011) Guide to Security for Full Virtualization Technologies. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-125. https://doi.org/10.6028/NIST.SP.800-125

[16] Wang Z, Jiang X (2010) Hypersafe: A lightweight approach to provide lifetime hypervisor control-flow integrity. *2010 IEEE Symposium on Security and Privacy (SP)* (IEEE, Berkeley/Oakland, CA), pp 380-395. https://doi.org/10.1109/SP.2010.30

[17] Berger S, Caceres R, Pendarakis D, Sailer R, Valdez E, Perez R, Schildhauer W, Srinivasan D (2008) TVDc: managing security in the trusted virtual datacenter. *ACM SIGOPS Operating Systems Review* 42(1):40-47. https://doi.org/10.1145/1341312.1341321

PUBLIKACJE ANGLOJĘZYCZNE[8]

[18] Sailer R, Valdez E, Jaeger T, Perez R, Doorn LV, Griffin JL, Berger S (2005) sHype:Secure hypervisor approach to trusted virtualized systems. (IBM Research Division, Yorktown Heights, NY) IBM Research Report RC23511. Available at https://domino.research.ibm.com/library/cyberdig.nsf/papers/265C8E3A6F95CA8D8525 6FA1005CBF0F/$File/rc23511.pdf

[19] Zhang Y, Juels A, Reiter MK, Ristenpart T (2014) Cross-tenant Side-channel Attacks in PaaS Clouds. *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (ACM, Scottsdale, AZ), pp 990-1003. https://doi.org/10.1145/2660267.2660356

[10] Osvik DA, Shamir A, Tromer E (2006) Cache attacks and countermeasures: the case of AES. Pointcheval D. (eds) Topics in Cryptology - CT-RSA 2006. CT-RSA 2006. Lecture Notes in Computer Science 3860 (Springer, Berlin), pp 1-20. https://doi.org/10.1007/11605805 1

[21] Tromer E,Osvik DA, Shamir A (2010) Efficient cache attacks on AES, and countermeasures. Journal of Cryptology 23(1): 37-71. https://doi.org/10.1007/s00145-009-9049-y

[22] Chandramouli R (2019) Security Strategies for Microservices-based Application Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-204. https://doi.org/10.6028/NIST.SP.800-204

[23] Yu S, Wang C, Ren K, Lou W (2010) Achieving secure, scalable, and fine-grained data access control in cloud computing. *INFOCOM, 2010 Proceedings* (IEEE, San Diego, CA), pp 1-9. https://doi.org/10.1109/INFCOM.2010.5462174

PUBLIKACJE ANGLOJĘZYCZNE[8]

[24] Hu VC, Ferraiolo DF, Kuhn DR, 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 02,2 019. https://doi.org/10.6028/NIST.SP.800-162

[25] Sahai A, Waters B (2005) Fuzzy identity-based encryption. *Advances in Cryptology - EUROCRYPT2005*. Lecture Notes in Computer Science 3494 (Springer, Berlin), pp 457- 473. https://doi.org/10.1007/11426639 27

26] Nali D, Adams CM, Miri A (2005) Using threshold attribute-based encryption for practical biometric-based access control. *International Journal of Network Security* 1(3):173-182.Available at http://iJns.Jalaxy.com.tw/download_paper.Jsp?PaperID=IJNS-2005-06-30-2&PaperName=iins-v1-n3/iins-2005-v1-n3-p173-182.pdf

[27] Zhu Y, Hu H, Ahn G-J, Huang D, Wang S (2012) Towards temporal access control in cloud computing. *INFOCOM, 2012 Proceedings* (IEEE, Orlando, FL), pp 2576-2580. https://doi.org/10.1109/INFCOM.2012.6195656

[28] Hu VC, Grance T, Ferraiolo DF, Kuhn DR (2014) An access control scheme for big data processing. *2014 International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom)* (IEEE, Miami, FL), pp 1-7. https://doi.org/10.4108/icst.collaboratecom.2014.257649

[29] Hu VC, Scarfone KA (2012) Guidelines for Access Control System Evaluation Metrics. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7874. https://doi.org/10.6028/NIST.IR.7874

PUBLIKACJE ANGLOJĘZYCZNE[8]

[30] Vipul G, Pandey O, Sahai A, Waters B (2006) Attribute-based encryption for fine-grained ccess control of encrypted data. *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06)* (ACM, Alexandria, VA), pp 89-98. https://doi.org/10.1145/1180405.1180418

[31] Hu VC, Kuhn DR, Ferraiolo DF, Voas J (2015) Attribute-based access control. *Computer* 48(2):85-88. http://doi.org/10.1109/MC.2015.33

[32] Sandhu RS, Coyne EJ, Feinstein HL, Youman CE (1996) Role-based access control models. *Computer* 29(2):38-47. https://doi.org/10.1109/2.485845

[33] Rubart J (2005) Context-based access control. Proceedings of the 2005 Symposia on Metainformatics (MIS '05). (ACM, New York, NY), pp 13-18. https://doi.org/10.1145/1234324.1234337

[34] Subashini S, Kavitha V (2011) A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications* 34(1), pp 1-11. https://doi.org/10.1016/i.jnca.2010.07.006

[35] Jin X, Krishnan R, Sandhu R (2012) A unified attribute-based access control model covering DAC, MAC, and RBAC. *Data and Applications Security and Privacy XXVI, DBSec 2012*. Lecture Notes in Computer Science 7371 (Springer, Berlin), pp 41-55. https://doi.org/10.1007/978-3-642-31540-4 4

[36] Decat M, Lagaisse B, Van Landuyt D, Crispo B, Joosen W (2013) Federated authorization for software-as-a-service applications. *On the Move to Meaningful Internet Systems: OTM 2013 Conferences*. Lecture Notes in Computer Science 8185 (Springer, Berlin), pp 342- 359. https://doi.org/10.1007/978-3-642-41030-7 25

PUBLIKACJE ANGLOJĘZYCZNE[8]

[37] Dimitrios Z, Lekkas D (2012) Addressing cloud computing security issues. Future Generation Computer Systems 28(3):583-592. https://doi.org/10.1016/j.future.2010.12.006

[38] McLean J (1985) A comment on the 'basic security theorem' of Bell and LaPadula. Information Processing Letters 20(2):67-70. https://doi.org/10.1016/0020-0190(85)90065-1

[39] Blobel B, Nordberg R, Davis JM, Pharow P (2006) Modelling privilege management and access control. *International Journal of Medical Informatics* 75(8), pp 597-623. https://doi.org/10.1016/j.ijmedinf.2005.08.010

[40] Bertino E, Federica P, Rodolfo F, Shang N (2009) Privacy-preserving digital identity anagement for cloud computing. *IEEE Data Engineering Bulletin* 32(1):21-27. Available t http://sites.computer.org/debull/A09mar/bertino.pdf

[41] Catteddu D (2010) Cloud Computing: Benefits, risks and recommendations for information security. *Web Application Security*. Communications in Computer and Information Science 72 (Springer, Berlin), pp 17-17. https://doi.org/10.1007/978-3-642-16120-9 9

[42] Simoijay F, Tierling E (2019) Shared Responsibility for Cloud Computing. (Microsoft, Redmond, WA), Version 2.0. Available at https://gallery.technet.microsoft.com/Shared-Responsibilities-81d0ff91/file/225366/1/Shared%20Responsibility%20for%20Cloud%20Computing-2019-10-25.pdf

ZAŁĄCZNIK A – WSKAZÓWKI W ZAKRESIE STOSOWALNOŚCI ZABEZPIECZEŃ KATEGORII AC

Poniższa tabela przedstawia wytyczne dotyczące kontroli dostępu do chmury wymienione w NSC 800-53 wer. 1, ***Zasady stosowania zabezpieczeń w systemach informacyjnych podmiotów publicznych***.

Tabela 4. Wykaz zabezpieczeń AC stosowanych w modelach IaaS, PaaS, SaaS.

Model	Wskazówka	Zabezpieczenie AC zawarte w NSC 800-53
IaaS	3.1 Wskazówka w zakresie sieci	AC-1, AC-3, AC-4, AC-5, AC-10, AC-17, AC-21, AC-22
	3.2 Wskazówka w zakresie hipernadzorcy	AC-1, AC-3, AC-5, AC-17, AC-21
	3.3 Wskazówka w zakresie maszyny wirtualnej (VM)	AC-1, AC-3, AC-4, AC-5, AC-11
	3.4 Wskazówka w zakresie API	AC-1, AC-3, AC-4, AC-5, AC-11, AC-17, AC-21, AC-22
PaaS	4.1 Wskazówka w zakresie pamięci danych	AC-1, AC-3, AC-4, AC-5, AC-10, AC-11, AC-21
	4.2 Wskazówka w zakresie API	AC-1, AC-3, AC-4, AC-5, AC-10, AC-11, AC 21
SaaS	5.1 Wskazówka dla właściciela danych	AC-1, AC-3, AC-5
	5.2 Wskazówka w zakresie poufności	AC-3, AC-6, AC-21
	5.3 Wskazówka w zakresie zarządzania przywilejami	AC-2, AC-11, AC-14, AC-22
	5.4 Wskazówka w zakresie replikacji danych	AC-1, AC-3, AC-4, AC-5, AC-17, AC-21
	5.5 Wskazówka w zakresie obsługi wielu podmiotów	AC-1, AC-2, AC-3, AC-4, AC-5, AC-10, AC-11, AC-21
	5.6 Wskazówka w zakresie zarządzania atrybutami i rolami	AC-6, AC-1, AC-3

Model	Wskazówka	Zabezpieczenie AC zawarte w NSC 800-53
SaaS	5.7 Wskazówka w zakresie polity	AC-1, AC-3
	5.8 Wskazówka w zakresie API	AC-1, AC-2, AC-3, AC-4, AC-5, AC-6, AC-11, AC-14, AC-17, AC-21

AC-1: Polityka i procedury kontroli dostępu

AC-2: Zarządzanie kontami

AC-3: Egzekwowanie uprawnień dostępu

AC-4: Egzekwowanie zasad przepływu informacji

AC-5: Rozdział obowiązków

AC-6: Zasada wiedzy koniecznej

AC-10: Kontrola ilości równoczesnych sesji

AC-11: Zamknięcie/blokada sesji

AC-14: Działania dozwolone bez identyfikacji lub uwierzytelnienia

AC-17: Dostęp zdalny

AC-21: Udostępnianie informacji

AC-22: Treści publicznie dostępne