Kancelaria Prezesa
Rady Ministrów

NARODOWY STANDARD CYBERBEZPIECZEŃSTWA
NSC 800-144 wer. 1.0

21 grudnia 2022

Wytyczne dotyczące bezpieczeństwa i prywatności w chmurze publicznej

Publikacja dostępna pod adresem:

Narodowe Standardy 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.

Prezentowana rekomendacja została opracowana na podstawie publikacji amerykańskiego National Institute of Science and Technology (NIST) na potrzeby dostawców, operatorów, brokerów, audytorów i odbiorców usług chmurowych oraz zarządzających tymi usługami, a także przedsiębiorców telekomunikacyjnych zapewniających łączność i dostęp do serwisów chmurowych.

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.

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

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

Niniejszy publikacja NSC 800-144, ***Wytyczne dotyczące bezpieczeństwa i prywatności w chmurze publicznej***, opracowana została za zgodą National Institute of Science and Technology (NIST) na podstawie specjalnej publikacji NIST SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing*.

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

Spis treści

Spis ilustracji

Spis tabel

STRESZCZENIE

Chmura obliczeniowa, przetwarzanie w chmurze (*ang. cloud computing*) to model przetwarzania danych oparty na użytkowaniu usług dostarczonych przez usługodawcę (wewnętrzny dział lub zewnętrzną organizację). Chmura obliczeniowa może oznaczać i oznacza różne rozwiązania dla wielu ludzi. Wspólną cechą większości interpretacji jest skalowalność na żądanie wysoce dostępnych i niezawodnych zasobów obliczeniowych, bezpieczny dostęp do usług z niemal dowolnego miejsca oraz przemieszczanie danych i usług z wewnątrz na zewnątrz organizacji. Chociaż niektóre z tych cech zostały w pewnym stopniu osiągnięte, chmura obliczeniowa pozostaje wciąż w fazie rozwoju. Niniejsza publikacja zawiera przegląd wyzwań związanych z bezpieczeństwem i prywatnością w publicznej chmurze obliczeniowej oraz wskazuje na czynniki, które organizacje powinny wziąć pod uwagę przy outsourcingu danych, aplikacji i infrastruktury do środowiska chmury publicznej.

PODSUMOWANIE ZARZĄDCZE

Chmura obliczeniowa została zdefiniowana przez National Institute of Standards and Technology (NIST) jako model umożliwiający wygodny, sieciowy dostęp na żądanie do współdzielonej puli konfigurowalnych zasobów obliczeniowych (np. sieci, serwerów, pamięci masowej, aplikacji i usług), które mogą być szybko dostarczane i uwalniane przy minimalnym wysiłku zarządzania lub interakcji z dostawcą chmury [Mel11][2]. Technologie chmury obliczeniowej mogą być wdrażane w szerokiej gamie architektur, w ramach różnych modeli usług i wdrożeń, a także mogą współistnieć z innymi technologiami i podejściami do projektowania oprogramowania. Wyzwania związane z bezpieczeństwem w chmurze obliczeniowej są ogromne, w tym te stojące przed chmurami publicznymi, których infrastruktura i zasoby obliczeniowe są własnością i są obsługiwane przez stronę zewnętrzną, która świadczy usługi dla ogółu społeczeństwa za pośrednictwem platformy wielodostępowej (*ang. multi-tenant platform*).

Pojawienie się chmury obliczeniowej zapowiada daleko idące skutki dla systemów i sieci organizacji. Wiele z cech, które czynią chmurę obliczeniową atrakcyjną, może być jednak również sprzecznych z tradycyjnymi modelami i środkami bezpieczeństwa. Podstawowym celem tej publikacji jest przedstawienie przeglądu publicznego przetwarzania w chmurze oraz związanych z nim rozważań na temat bezpieczeństwa i ochrony prywatności. Niniejszy dokument opisuje zagrożenia, ryzyka technologiczne i zabezpieczenia otaczające środowiska chmur publicznych oraz ich omówienie. Wytyczne te nie nakazują, ani nie zalecają żadnej konkretnej usługi chmury obliczeniowej, umowy o świadczenie usług, dostawcy usług lub modelu wdrożenia. Od każdej organizacji oczekuje się natomiast zastosowania przedstawionych wytycznych podczas przeprowadzania własnej analizy swoich wymagań oraz oceny, wyboru,

[2] Numery w nawiasach kwadratowych odnoszą się do stosownych publikacji zawartych w Referencjach (dotyczy to całego dokumentu).

zaangażowania i nadzorowania usług chmury publicznej, które mogą najlepiej spełnić te wymagania.

Kluczowe wytyczne są podsumowane i wymienione poniżej i są zalecane dla organizacji publicznych i sektora prywatnego.

Dokładne zaplanowanie aspektów bezpieczeństwa i ochrony prywatności w zakresie rozwiązań przetwarzania w chmurze przed ich wprowadzeniem.

Publiczna chmura obliczeniowa reprezentuje znaczącą zmianę paradygmatu z konwencjonalnych norm organizacyjnego centrum danych na zdepersonalizowaną infrastrukturę otwartą na wykorzystanie przez potencjalnych adwersarzy. Jak w przypadku każdego nowego obszaru technologii informacyjnej, do przetwarzania w chmurze należy podchodzić ostrożnie, z należytym uwzględnieniem wrażliwości danych. Planowanie pomaga zapewnić, że środowisko obliczeniowe jest tak bezpieczne, jak to tylko możliwe i zgodne ze wszystkimi odpowiednimi politykami organizacyjnymi oraz, że zachowana jest prywatność. Pomaga również zapewnić, że organizacja czerpie pełne korzyści z wydatków poniesionych na technologie informatyczne.

Cele bezpieczeństwa organizacji są kluczowym czynnikiem przy podejmowaniu decyzji o outsourcingu usług informatycznych, a w szczególności przy podejmowaniu decyzji o przeniesieniu danych organizacyjnych, aplikacji i innych zasobów do środowiska publicznej chmury obliczeniowej. Organizacje powinny przyjąć podejście oparte na ryzyku przy analizowaniu dostępnych opcji bezpieczeństwa i ochrony prywatności oraz podejmowaniu decyzji o umieszczeniu funkcji organizacyjnych w środowisku chmury. Praktyki zarządzania technologiami informacyjnymi organizacji, które odnoszą się do polityk, procedur i standardów wykorzystywanych do rozwoju aplikacji i dostarczania usług, jak również projektowania, wdrażania, testowania, korzystania i monitorowania wdrożonych lub zaangażowanych usług, powinny być rozszerzone na środowiska przetwarzania w chmurze.

W celu maksymalizacji efektywności i minimalizacji kosztów, bezpieczeństwo i prywatność muszą być brane pod uwagę przez cały cykl życia systemu, od początkowego etapu planowania. Próba rozwiązania problemów związanych

z bezpieczeństwem i ochroną prywatności po implementacji i wdrożeniu jest nie tylko znacznie trudniejsza i kosztowniejsza, ale także naraża organizację na niepotrzebne ryzyko.

Poznanie środowiska przetwarzania w chmurze publicznej oferowanego przez dostawcę usług chmurowych.

Obowiązki zarówno organizacji jak i dostawcy usług chmurowych różnią się w zależności od modelu usługi. Organizacje korzystające z usług w chmurze muszą rozumieć rozgraniczenie odpowiedzialności nad środowiskiem przetwarzania oraz implikacje dla bezpieczeństwa i prywatności. Gwarancje wiarygodności złożone przez dostawcę usługi w chmurze na poparcie roszczeń dotyczących bezpieczeństwa lub prywatności, lub przez podmiot zajmujący się certyfikacją i przeglądem zgodności opłacany przez dostawcę usługi w chmurze, powinny być weryfikowane, gdy tylko jest to możliwe, poprzez niezależną ocenę organizacji.

Zrozumienie polityk, procedur i zabezpieczeń technicznych stosowanych przez dostawcę usług w chmurze jest warunkiem wstępnym do oceny ryzyka związanego z bezpieczeństwem i ochroną prywatności. Ważne jest również zrozumienie technologii wykorzystywanych do świadczenia usług i ich implikacji dla bezpieczeństwa i prywatności w systemie. Szczegóły dotyczące architektury systemu chmury mogą być analizowane i wykorzystywane do sformułowania pełnego obrazu ochrony zapewnianej przez środki bezpieczeństwa i ochrony prywatności, co zwiększa zdolność organizacji do dokładnej oceny i zarządzania ryzykiem, w tym ograniczania ryzyka poprzez stosowanie odpowiednich technik i procedur ciągłego monitorowania stanu bezpieczeństwa systemu.

Upewnienie się, że rozwiązanie przetwarzania w chmurze spełnia wymagania organizacyjne w zakresie bezpieczeństwa i ochrony prywatności.

Domyślne oferty dostawców chmury publicznej zazwyczaj nie odzwierciedlają potrzeb konkretnej organizacji w zakresie bezpieczeństwa i ochrony prywatności. Z perspektywy ryzyka, określenie przydatności usług w chmurze wymaga zrozumienia kontekstu, w którym działa organizacja oraz konsekwencji wynikających z prawdopodobnych zagrożeń, przed którymi stoi. Dostosowania do środowiska

przetwarzania w chmurze mogą być uzasadnione w celu spełnienia wymagań organizacji. Organizacje powinny wymagać, aby każde wybrane rozwiązanie publicznej chmury obliczeniowej było skonfigurowane, wdrożone i zarządzane w celu spełnienia ich wymagań w zakresie bezpieczeństwa, ochrony prywatności i innych.

Nienegocjowane umowy o świadczenie usług, w których warunki ich świadczenia są całkowicie określone przez dostawcę chmury, są ogólnie normą w publicznym przetwarzaniu w chmurze. Dostępne są również negocjowane umowy o świadczenie usług. Podobnie jak tradycyjne kontrakty na outsourcing technologii informacyjnych stosowane przez agencje, negocjowane umowy mogą uwzględniać kwestie bezpieczeństwa i prywatności organizacji, takie jak weryfikacja pracowników, prawa własności i wycofania danych, powiadamianie o naruszeniach, izolacja aplikacji dzierżawionych, szyfrowanie i segregacja danych, śledzenie i raportowanie efektywności usług, zgodność z prawami i regulacjami oraz wykorzystanie zatwierdzonych produktów spełniających standardy organizacyjne lub krajowe (*np. Federal Information Processing Standard 140*). Wynegocjowana umowa może również dokumentować gwarancje, które dostawca chmury musi przedstawić, aby potwierdzić, że wymagania organizacyjne są spełnione.

Krytyczne dane i aplikacje mogą wymagać od organizacji zawarcia negocjowanej umowy o świadczenie usług w celu korzystania z chmury publicznej. Negocjowanie warunków może negatywnie wpłynąć na ekonomikę skali, którą nienegocjowana umowa o świadczenie usług wnosi do publicznego przetwarzania w chmurze, sprawiając jednak, że negocjowana umowa jest mniej opłacalna. Alternatywnie, organizacja może zastosować zabezpieczenia kompensacyjne, aby zminimalizować zidentyfikowane słabości usługi w chmurze publicznej. Inne alternatywy obejmują środowiska przetwarzania w chmurze z zastosowaniem bardziej dopasowanego modelu wdrożenia, takiego jak wewnętrzna chmura prywatna, która może potencjalnie zaoferować organizacji większy nadzór i kontrolę nad bezpieczeństwem i prywatnością oraz lepiej ograniczyć kategorie dzierżawców, którzy współdzielą zasoby platformy, zmniejszając ekspozycję w przypadku awarii lub błędu konfiguracji zabezpieczeń.

Wraz z rosnącą liczbą dostawców usług w chmurze i zakresem usług, z których można korzystać, organizacje muszą zachować należytą staranność przy wyborze i przenoszeniu działalności do chmury. Podejmowanie decyzji dotyczących usług i umów o świadczenie usług wiąże się z koniecznością znalezienia równowagi pomiędzy korzyściami w zakresie kosztów i wydajności, a wadami w zakresie ryzyka i odpowiedzialności. Podczas gdy wrażliwość danych przetwarzanych przez organizacje rządowe oraz obecny stan techniki sprawiają, że prawdopodobieństwo outsourcingu wszystkich usług informatycznych do chmury publicznej jest niskie, dla większości organizacji rządowych powinno być możliwe wdrożenie niektórych usług informatycznych do rządowej chmury obliczeniowej, pod warunkiem, że podjęte zostaną wszystkie wymagane środki ograniczające ryzyko.

Zapewnienie, że środowisko obliczeniowe po stronie klienta spełnia wymagania organizacyjne w zakresie bezpieczeństwa i prywatności dla chmury obliczeniowej.

Chmura obliczeniowa obejmuje zarówno stronę serwerową, jak i kliencką. Przy nacisku kładzionym zazwyczaj na tę pierwszą, drugą można łatwo przeoczyć. Usługi od różnych dostawców chmury, jak również aplikacje oparte na chmurze stworzone przez organizację, mogą nakładać bardziej wymagające wymagania na klienta, co może mieć wpływ na bezpieczeństwo i prywatność, które należy wziąć pod uwagę.

Ze względu na ich wszechobecność, przeglądarki internetowe są kluczowym elementem dostępu po stronie klienta do usług chmury obliczeniowej. Klienci mogą również korzystać z małych, lekkich aplikacji, które działają na urządzeniach stacjonarnych i mobilnych, aby uzyskać dostęp do usług. Różne dostępne wtyczki i rozszerzenia do przeglądarek internetowych są notorycznie narażone na problemy związane z bezpieczeństwem. Wiele dodatków do przeglądarek nie zapewnia również automatycznych aktualizacji, co zwiększa trwałość istniejących luk w zabezpieczeniach (podatności). Podobne problemy występują w przypadku innych typów klientów.

Utrzymanie fizycznego i logicznego bezpieczeństwa na poziomie klientów może być kłopotliwe, szczególnie w przypadku zintegrowanych urządzeń mobilnych, takich jak smartfony. Ich rozmiar i przenośność mogą powodować utratę fizycznej kontroli. Wbudowane mechanizmy bezpieczeństwa często nie są wykorzystywane lub mogą być

bez trudu pokonane lub ominięte przez kompetentną osobę w celu przejęcia kontroli nad urządzeniem. Ponadto, aplikacje w chmurze są często dostarczane do nich za pośrednictwem specjalnie stworzonych aplikacji natywnych (tj. programów, apps), a nie przeglądarki internetowej.

Rosnąca dostępność i korzystanie z mediów społecznościowych, osobistej poczty internetowej i innych publicznie dostępnych stron staje się zagrożeniem, ponieważ coraz częściej służą one jako miejsca ataków socjotechnicznych, które mogą negatywnie wpłynąć na bezpieczeństwo klienta, jego platformy bazowej i udostępnianych usług w chmurze. Istnienie „tylnej furtki" (*ang. backdoor*), trojana, rejestratora naciśnięć klawiszy lub innego rodzaju złośliwego oprogramowania działającego na urządzeniu klienckim podważa bezpieczeństwo i prywatność usług chmury publicznej, a także innych publicznie dostępnych usług internetowych. W ramach ogólnej architektury bezpieczeństwa przetwarzania w chmurze, organizacje powinny dokonać przeglądu istniejących środków bezpieczeństwa i ochrony prywatności oraz zastosować dodatkowe zabezpieczenia, jeśli jest to konieczne, aby skutecznie chronić stronę klienta.

Utrzymanie odpowiedzialności za prywatność i bezpieczeństwo danych i aplikacji wdrożonych i rozmieszczonych w publicznych środowiskach przetwarzania chmurowego.

Organizacje powinny stosować odpowiednie praktyki zarządzania bezpieczeństwem i zabezpieczeniami w środowisku przetwarzania chmurowego. Skuteczne praktyki zarządzania są niezbędne do obsługi i utrzymania bezpiecznego rozwiązania przetwarzania w chmurze. Praktyki bezpieczeństwa i ochrony prywatności obejmują monitorowanie aktywów systemu informacyjnego organizacji oraz ocenę wdrożenia polityk, standardów, procedur, zabezpieczeń i wytycznych, które są wykorzystywane do ustanowienia i zachowania poufności, integralności i dostępności zasobów systemu informacyjnego.

Organizacja powinna zbierać i analizować dostępne dane o stanie systemu regularnie i tak często, jak jest to potrzebne do zarządzania ryzykiem związanym z bezpieczeństwem i prywatnością, odpowiednio dla każdego poziomu organizacji (tj.

poziomu zarządzania, poziomu misji lub procesu biznesowego oraz poziomu systemów informacyjnych) [Dem10]. Ciągłe monitorowanie bezpieczeństwa informacji wymaga utrzymywania stałej świadomości zabezpieczeń prywatności i bezpieczeństwa, podatności i zagrożeń w celu wspierania decyzji dotyczących zarządzania ryzykiem. Celem jest prowadzenie ciągłego monitorowania bezpieczeństwa sieci, informacji i systemów organizacji oraz reagowanie poprzez akceptowanie, unikanie lub ograniczanie ryzyka w miarę zmian sytuacji.

Ocena i zarządzanie ryzykiem w systemach chmur obliczeniowych może być wyzwaniem, ponieważ znaczące części środowiska obliczeniowego są pod kontrolą dostawcy chmury i mogą znajdować się poza zasięgiem organizacji. W analizie ryzyka mają zastosowanie zarówno czynniki jakościowe, jak i ilościowe. Ryzyko musi być starannie wyważone w stosunku do dostępnych zabezpieczeń technicznych, zarządczych i operacyjnych oraz muszą być podjęte niezbędne kroki, aby zredukować ryzyko do akceptowalnego poziomu. Organizacja musi również zapewnić, że środki bezpieczeństwa i ochrony prywatności są prawidłowo wdrożone, działają zgodnie z przeznaczeniem i spełniają wymagania organizacyjne.

Ustanowienie poziomu zaufania do środowiska usług w chmurze zależy od zdolności dostawcy chmury do zapewnienia środków bezpieczeństwa niezbędnych do ochrony danych i aplikacji organizacji, a także od dostarczonych dowodów na skuteczność tych zabezpieczeń [JTF10]. Weryfikacja poprawności działania podsystemu i skuteczności środków bezpieczeństwa w tak szerokim zakresie jak w przypadku wewnętrznego systemu organizacyjnego może być jednak w niektórych przypadkach niewykonalna, a do ustalenia poziomu zaufania można wykorzystać inne czynniki, takie jak audyty stron trzecich. Ostatecznie, jeśli poziom zaufania do usługi spadnie poniżej oczekiwań, a organizacja nie jest w stanie zastosować zabezpieczeń kompensacyjnych, musi albo odrzucić usługę, albo zaakceptować większy stopień ryzyka.

Bezpieczeństwo chmury obliczeniowej zależy od bezpieczeństwa wielu pojedynczych komponentów. Oprócz komponentów do obliczeń ogólnych, istnieją również komponenty, z których składa się płaszczyzna zarządzania, takie jak komponenty do samoobsługi, pomiaru zasobów, zarządzania kwotami, replikacji i odzyskiwania danych,

monitorowania poziomu usług i zarządzania obciążeniem pracą. Wiele uproszczonych interfejsów i abstrakcji usług oferowanych przez chmurę obliczeniową świadczy o nieodłącznej złożoności, która wpływa na bezpieczeństwo. Organizacje powinny zapewnić w maksymalnym możliwym stopniu, że wszystkie elementy chmury obliczeniowej są bezpieczne oraz że bezpieczeństwo i prywatność są utrzymywane w oparciu o solidne praktyki obliczeniowe[3]. Standardy i przewodniki wymienione w poniższej tabeli zawierają materiały, które są szczególnie istotne dla chmury obliczeniowej i powinny być wykorzystywane w połączeniu z niniejszą publikacją.

Tabela 1. Polecane standardy i przewodniki.

Publikacja	Tytuł
NSC 199	Standardy kategoryzacji bezpieczeństwa.
NSC 200	Minimalne wymogi bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych.
NSC 800-18	Przewodnik do opracowywania planów bezpieczeństwa systemów informacyjnych w podmiotach publicznych.
NSC 800-34	Poradnik planowania awaryjnego.
NSC 800-37	Ramy zarządzania ryzykiem w organizacjach i systemach informacyjnych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu.
NSC 800-39	Zarządzanie ryzykiem bezpieczeństwa informacji. Przegląd struktury organizacyjnej, misji i systemu informacyjnego.

[3] Np. nakreślone w Federalnych Standardach Przetwarzania Informacji (FIPS), Specjalnych Publikacjach NIST (NIST SP) oraz Narodowych Standardach Cyberbezpieczeństwa (NSC).

Publikacja	Tytuł
NSC 800-53	Zabezpieczenia i ochrona prywatności w systemach informacyjnych oraz organizacjach.
NSC 800-53A	Ocenianie środków bezpieczeństwa i ochrony prywatności w systemach informacyjnych oraz organizacjach. Tworzenie skutecznych planów oceny.
NSC 800-53B	Zabezpieczenia bazowe systemów informacyjnych oraz organizacji.
NSC 800-60	Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informacyjnego.
NSC 800-61	Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego.
NIST SP 800-64	Security Considerations in the System Development Life Cycle.
NIST SP 800-86	Guide to Integrating Forensic Techniques into Incident Response.
NIST SP 800-88	Guidelines for Media Sanitization.
NIST SP 800-115	Technical Guide to Information Security Testing and Assessment.
NIST SP 800-122	Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).
NIST SP 800-137	Information Security Continuous Monitoring for Federal Information Systems and Organizations,

1. WSTĘP

Zainteresowanie chmurą obliczeniową gwałtownie wzrosło w ostatnich latach ze względu na korzyści wynikające z większej elastyczności i dostępności w pozyskiwaniu zasobów obliczeniowych po niższych kosztach. Bezpieczeństwo i prywatność, jednakże, są obiektem szczególnego zainteresowania organizacji, które rozważają przeniesienie aplikacji i danych do środowisk chmury publicznej i stanowią podstawę do opracowania tego dokumentu.

1.1. UPRAWNIENIA[4]

Narodowy Instytut Standardów i Technologii (*ang. National Institute of Standards and Technology - NIST*) opracował ten dokument w ramach swoich ustawowych obowiązków wynikających z Federal Information Security Management Act (FISMA) z 2002 r., Public Law 107-347.

NIST jest odpowiedzialny za opracowywanie norm i wytycznych, w tym minimalnych wymagań, w celu zapewnienia odpowiedniego poziomu bezpieczeństwa informacji wszystkich operacji i aktywów organizacji; takie normy i wytyczne nie mają jednak zastosowania do systemów bezpieczeństwa narodowego. Niniejsze wytyczne są zgodne z wymogami Okólnika A-130 Biura Zarządzania i Budżetu (*ang. Office of Management and Budget - OMB*), sekcja 8b(3), "Zabezpieczanie systemów informacyjnych agencji", co zostało przeanalizowane w A-130, Dodatek IV: Analiza kluczowych sekcji. Informacje uzupełniające znajdują się w A-130, Dodatek III.

Niniejsze wytyczne zostały przygotowane do użytku przez organizacje publiczne. Mogą być wykorzystywany przez organizacje pozarządowe na zasadzie dobrowolności i nie podlegają prawom autorskim, choć pożądane jest umieszczenie w nim informacji o źródle.

[4] Sekcja ta nie dotyczy rynku polskiego. Została podana jako przykład dla zainteresowanych, chcących poszerzyć swoją wiedzę.

Żaden z zapisów niniejszego dokumentu nie powinien być traktowany, jako sprzeczny ze standardami i wytycznymi, które stały się obowiązkowe i wiążące dla agencji federalnych przez Sekretarza Handlu na mocy upoważnienia ustawowego, ani też niniejsze wytyczne nie powinny być interpretowane, jako zmieniające lub zastępujące istniejące uprawnienia Sekretarza Handlu (*ang. Secretary of Commerce*), Dyrektora OMB lub jakiegokolwiek innego urzędnika federalnego.

1.2. CEL I ZAKRES

Celem tego dokumentu jest przedstawienie zarysu przetwarzania w chmurze publicznej oraz związanych z tym wyzwań w zakresie bezpieczeństwa i ochrony prywatności. Dokument omawia zagrożenia, ryzyka technologiczne i zabezpieczenia dla środowisk chmur publicznych oraz dostarcza wiedzy umożliwiającej podejmowanie świadomych decyzji dotyczących technologii informatycznych w zakresie ich wykorzystania. Dokument ten nie nakazuje ani nie zaleca żadnej konkretnej usługi przetwarzania w chmurze, umowy o świadczenie usług, dostawcy usług lub modelu wdrożenia. Każda organizacja musi przeprowadzić własną analizę swoich potrzeb oraz ocenić, wybrać, wdrożyć i nadzorować usługi chmury publicznej, które najlepiej zaspokoją te potrzeby.

1.3. ODBIORCY

Docelowi odbiorcy tego dokumentu obejmują następujące kategorie osób:

- Menedżerowie systemów, kadra kierownicza i personel podejmujący decyzje dotyczące realizacji przedsięwzięć związanych z chmurą obliczeniową.
- Profesjonaliści ds. bezpieczeństwa, w tym personel bezpieczeństwa, administratorzy bezpieczeństwa, audytorzy i inne osoby odpowiedzialne za bezpieczeństwo technologii informacyjnych.
- Kierownicy programów informatycznych zaangażowani w środki bezpieczeństwa i ochrony prywatności w chmurze obliczeniowej.
- Administratorzy systemów i sieci.
- Użytkownicy publicznych usług przetwarzania w chmurze.

Dokument, mimo że ma charakter techniczny, zawiera informacje ogólne, które pomogą zainteresowanym osobom zrozumieć poruszane w nim tematy. Materiał ten zakłada, że czytelnicy posiadają podstawową wiedzę na temat systemów operacyjnych i sieci oraz podstawowe zrozumienie przetwarzania w chmurze. Ze względu na ewoluujący charakter kwestii bezpieczeństwa i ochrony prywatności w chmurze obliczeniowej, oczekuje się, że czytelnicy skorzystają z innych źródeł w celu uzyskania bardziej szczegółowych i aktualnych informacji. Zasoby te obejmują różne publikacje wymienione lub przywołane w tym dokumencie, z których większość jest dostępna on-line.

1.4. STRUKTURA DOKUMENTU

Pozostała część niniejszego dokumentu została podzielona na następujące rozdziały:

- Rozdział 2 przedstawia przegląd publicznych chmur obliczeniowych.
- Rozdział 3 omawia korzyści i wady usług chmury publicznej z perspektywy bezpieczeństwa i ochrony prywatności.
- Rozdział 4 omawia kluczowe problemy w zakresie bezpieczeństwa i ochrony prywatności w publicznej chmurze obliczeniowej oraz środki ostrożności, które można podjąć w celu ich zredukowania.
- Rozdział 5 zawiera wskazówki dotyczące rozwiązywania problemów dotyczących bezpieczeństwa i ochrony prywatności podczas powierzania obsługi danych i aplikacji dostawcy usług chmurowych.
- Rozdział 6 zawiera krótkie podsumowanie.
- Rozdział 7 zawiera wykaz literatury.

Materiały pomocnicze związane z główną dyskusją pojawiają się w szarych polach tekstowych w głównej części dokumentu. Na końcu dokumentu znajdują się również załączniki, które zawierają materiały pomocnicze: Lista akronimów znajduje się w Załączniku A, a lista zasobów internetowych znajduje się w Załączniku B.

2. INFORMACJE OGÓLNE[5]

Chmura obliczeniowa został zdefiniowany przez NIST, jako model umożliwiający wygodny, sieciowy dostęp na żądanie do współdzielonej puli konfigurowalnych zasobów obliczeniowych (np. sieci, serwerów, pamięci masowej, aplikacji i usług), które mogą być szybko dostarczane i uwalniane przy minimalnym wysiłku zarządzania lub interakcji z dostawcą chmury [Mel11]. Chmura obliczeniowa może być uważana za nowy paradygmat obliczeniowy, o ile pozwala na wykorzystanie infrastruktury obliczeniowej na jednym lub kilku poziomach abstrakcji, jako usługi na żądanie udostępnianej przez Internet lub inną sieć komputerową. Ze względu na implikacje związane z większą elastycznością i dostępnością przy niższych kosztach, chmura obliczeniowa jest tematem, któremu poświęca się wiele uwagi.

Usługi w chmurze obliczeniowej korzystają z ekonomii skali osiąganej dzięki wszechstronnemu wykorzystaniu zasobów, specjalizacji i innym możliwym do zastosowania usprawnieniom. Jednak chmura obliczeniowa jest rozwijającą się formą przetwarzania rozproszonego, która wciąż podlega ewolucji i standaryzacji. Sam termin jest dziś często używany z wieloma znaczeniami i interpretacjami [Fow09]. Wiele z tego, co zostało napisane o chmurze obliczeniowej jest definicyjne, ma na celu zidentyfikowanie ważnych paradygmatów wdrażania i użytkowania oraz zapewnienie ogólnej taksonomii do pojęciowego opisania istotnych aspektów usługi.

2.1. MODELE WDROŻENIOWE

Publiczna chmura obliczeniowa jest jednym ze zdefiniowanych modeli wdrażania [Mel11]. Modele wdrożeniowe w ogólny sposób charakteryzują zarządzanie i udostępnianie zasobów obliczeniowych w celu dostarczenia usług odbiorcom usług chmurowych, jak również wprowadzają podział na klasy odbiorców. Chmura publiczna to taka, w której infrastruktura i zasoby obliczeniowe, z których się składa, są udostępniane ogółowi społeczeństwa przez Internet. Jest ona własnością i jest

[5] Patrz – NSC 500-292

zarządzana przez dostawcę chmury dostarczającego usługi w chmurze odbiorcom i z założenia jest to zewnętrzna organizacja w stosunku do odbiorców. Szczególnym przypadkiem są chmury prywatne. Chmura prywatna to taka, w której środowisko obliczeniowe jest obsługiwane wyłącznie dla jednej organizacji. Może być zarządzana przez tę organizację lub przez stronę trzecią i może być hostowana w centrum danych organizacji lub poza nim. Chmura prywatna może potencjalnie zapewnić organizacji lepszą kontrolę nad infrastrukturą, zasobami obliczeniowymi i odbiorcami usług chmurowych niż chmura publiczna.

Istnieją również dwa inne modele wdrażania: chmury wspólnotowe i hybrydowe. Chmura wspólnotowa znajduje się pomiędzy chmurami publicznymi i prywatnymi w odniesieniu do docelowej grupy odbiorców. Jest ona podobna do chmury prywatnej, ale infrastruktura i zasoby obliczeniowe są przeznaczone wyłącznie dla dwóch lub więcej organizacji, które mają wspólne względy dotyczące prywatności, bezpieczeństwa i przepisów, a nie dla pojedynczej organizacji.[6] Chmury hybrydowe są bardziej złożone niż inne modele wdrażania, ponieważ obejmują kompozycję dwóch lub więcej chmur (prywatnych, społecznościowych lub publicznych). Każdy uczestnik pozostaje unikalną jednostką, ale jest powiązany z innymi za pomocą znormalizowanej lub własnościowej technologii, która umożliwia przenoszenie aplikacji i danych między nimi.

Chociaż wybór modelu wdrażania ma wpływ na bezpieczeństwo i prywatność w systemie, sam model wdrażania nie określa poziomu bezpieczeństwa i ochrony prywatności konkretnych ofert w chmurze. Poziom ten zależy głównie od zapewnienia, takiego jak trafność ustanowionych polityk bezpieczeństwa i prywatności, solidność stosowanych środków bezpieczeństwa i ochrony prywatności oraz stopień przejrzystości szczegółów dotyczących wydajności i zarządzania środowiskiem chmury, które są dostarczane przez dostawcę chmury lub są uzyskiwane niezależnie

[6] Termin "organizacja" jest używany równoznacznie z terminem "odbiorca chmury" w całej tej publikacji.

przez organizację (np. poprzez samodzielne badanie podatności lub audyt funkcjonowania).

2.2. MODELE USŁUG

Tak jak modele wdrożenia pełnią ważną rolę w chmurze obliczeniowej, modele usług stanowią również istotną kwestię. Model usługi, do którego dopasowana jest usługa w chmurze, dyktuje zakres i kontrolę organizacji nad środowiskiem obliczeniowym oraz charakteryzuje poziom abstrakcji jego wykorzystania. Model usługowy może być zrealizowany, jako chmura publiczna lub jako którykolwiek z pozostałych modeli wdrożeniowych. Trzy znane i najczęściej stosowane modele usług to [Lea09, Mel11, Vaq09, You08]:

- **Oprogramowanie jako usługa (*ang. Software-as-a-Service - SaaS*)** - model usługi chmurowej umożliwiający odbiorcy usług chmurowych wykorzystanie aplikacji uruchomionych na infrastrukturze chmury dostarczanej przez dostawcę usług chmurowych, dostępnych na różnych urządzeniach klienckich za pośrednictwem np. przeglądarki internetowej lub klienta aplikacji oraz w przypadku której odbiorca usług nie zarządza ani nie kontroluje infrastruktury chmury, w tym sieci, serwerów, systemów operacyjnych, pamięci masowej, a nawet parametrów konfiguracyjnych aplikacji, z wyjątkiem ograniczonych ustawień konfiguracji aplikacji specyficznych dla użytkownika.
- **Platforma jako usługa (*ang. Platform as a service – PaaS*)** - model usługi chmurowej umożliwiający odbiorcy usług chmurowych wdrożenie na infrastrukturze chmury aplikacji stworzonych przez siebie lub nabytych, które zostały przygotowane przy użyciu języków programowania, bibliotek, usług i narzędzi obsługiwanych przez dostawcę, w przypadku której odbiorca usług nie zarządza ani nie kontroluje infrastruktury chmury, w tym sieci, serwerów, systemów operacyjnych oraz pamięci masowych, ale ma kontrolę nad wdrożonymi aplikacjami i, ewentualnie, nad ustawieniami konfiguracji dla środowiska udostępnienia aplikacji.
- **Infrastruktura jako usługa (*ang. Infrastructure-as-a-Service - IaaS*)** - model usługi chmurowej zapewniający infrastrukturę chmury, na której odbiorca usług chmurowych jest w stanie wdrożyć i uruchomić dowolne oprogramowanie

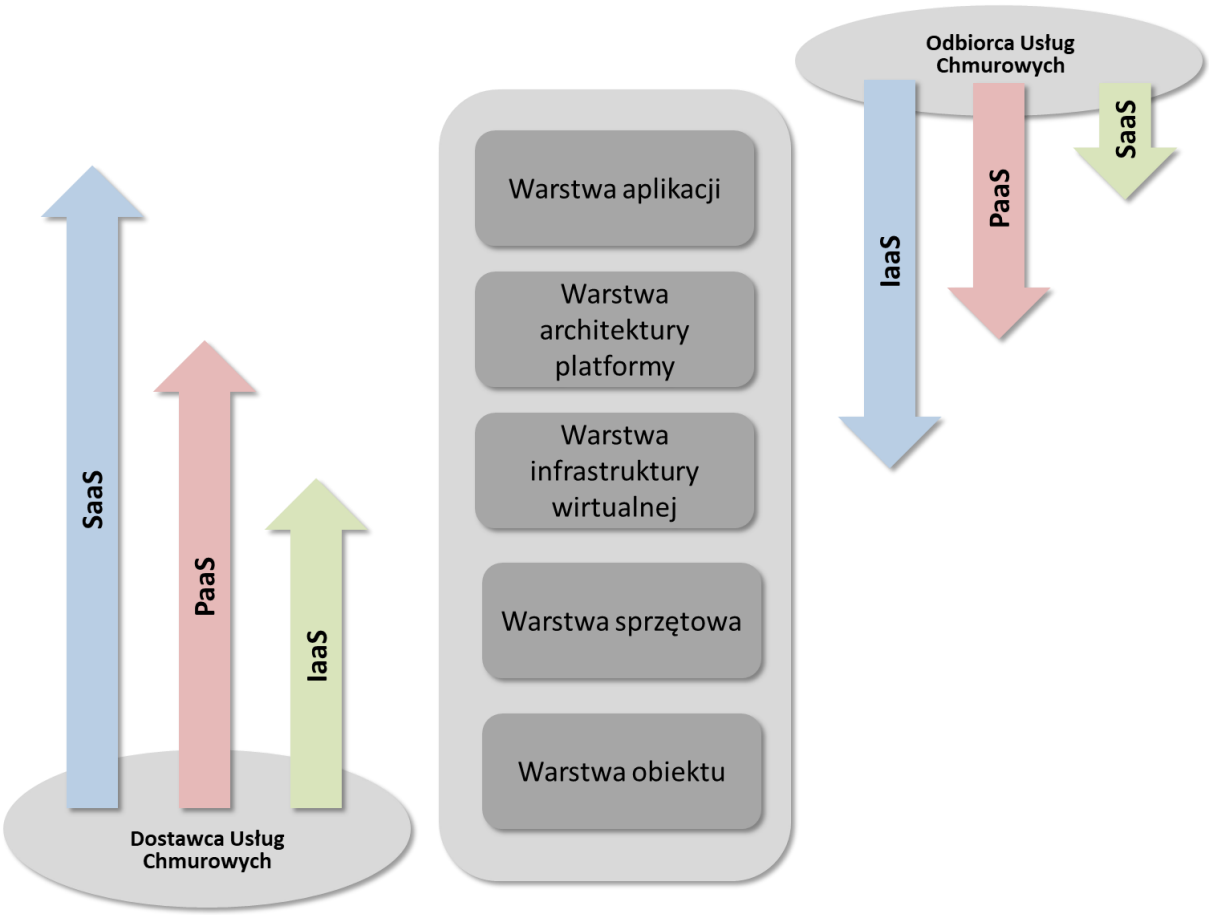
(systemy operacyjne i aplikacje), jednak nie zarządza ani nie kontroluje infrastruktury chmury, z wyjątkiem kontroli nad systemami operacyjnymi, pamięcią masową i wdrożonymi aplikacjami oraz, ewentualnie, ograniczonej kontroli nad wybranymi komponentami sieciowymi (np. zapór sieciowych).

Rysunek 1 ilustruje różnice w zakresie odpowiedzialności i kontroli między konsumentem usługi chmurowej, a dostawcą chmury dla każdego z modeli usług omówionych powyżej. Pięć pojęciowych warstw uogólnionego środowiska chmury jest zidentyfikowanych na środkowym diagramie i ma zastosowanie do chmur publicznych, jak również każdego z pozostałych modeli wdrożenia. Strzałki po lewej i prawej stronie diagramu oznaczają przybliżony zakres odpowiedzialności oraz kontroli przez dostawcę i odbiorcę usługi w chmurze nad środowiskiem chmury dla każdego modelu usługi. Ogólnie rzecz biorąc, im wyższy poziom wsparcia dostępny od dostawcy chmury, tym węższy jest zakres i kontrola, jaką odbiorca usług chmurowych ma nad systemem.

Dwie najniższe pokazane warstwy oznaczają fizyczne elementy środowiska chmury, które są pod pełną kontrolą dostawcy chmury, niezależnie od modelu usług. Ogrzewanie, wentylacja, klimatyzacja (*ang. heating, ventilation, air conditioning - HVAC*), zasilanie, teletransmisja i inne aspekty fizycznej instalacji tworzą dolną warstwę, *Warstwę obiektu*, podczas gdy komputery, elementy sieci i pamięci masowej oraz inne elementy fizycznej infrastruktury obliczeniowej tworzą *Warstwę sprzętową* bezpośrednio ulokowaną nad nią.

Pozostałe warstwy oznaczają logiczne elementy środowiska chmury. *Warstwa infrastruktury wirtualnej* obejmuje elementy oprogramowania, takie jak hiperwizory, maszyny wirtualne, wirtualne przechowywanie danych oraz wirtualne komponenty sieciowe wykorzystywane do realizacji infrastruktury, na której można utworzyć platformę obliczeniową. Podczas gdy technologia maszyn wirtualnych jest powszechnie stosowana w tej warstwie, nie wyklucza się innych środków zapewniających niezbędne abstrakcje oprogramowania. Podobnie, *warstwa architektury platformy* obejmuje kompilatory, biblioteki, programy narzędziowe, oprogramowanie pośredniczące i inne narzędzia programowe oraz składniki programistyczne potrzebne

do wdrażania i rozmieszczania aplikacji. *Warstwa aplikacji* reprezentuje wdrożone aplikacje programowe, które są przeznaczone dla oprogramowania klienckiego użytkownika końcowego lub innych programów i udostępniane za pośrednictwem chmury.



Rysunek 1. Różnice w zakresie odpowiedzialności i kontroli pomiędzy modelami usług w chmurze.

Istnieją argumenty, że rozróżnienie między modelami usług IaaS i PaaS jest nieostre, a w wielu komercyjnych ofertach te dwa modele są do siebie bardziej podobne niż rozbieżne [Arm10]. Niemniej jednak terminy te służą określonemu celowi, wyróżniając bardzo podstawowe środowiska wsparcia i środowiska o większym poziomie wsparcia, oraz odpowiednio różne alokacje kontroli i odpowiedzialności pomiędzy odbiorcą usług chmurowych, a dostawcą chmury.

2.3. PODWYKONAWSTWO I ODPOWIEDZIALNOŚĆ

Podczas, gdy przetwarzanie w chmurze może być wdrożone wyłącznie na potrzeby organizacji jako wewnątrzorganizacyjna chmura prywatna, jego główną ideą jest zapewnienie narzędzia do outsourcingu części organizacyjnego środowiska obliczeniowego na zewnątrz za pośrednictwem chmury publicznej. Jak w przypadku każdego outsourcingu usług informatycznych, istnieją obawy dotyczące skutków w zakresie bezpieczeństwa komputerowego i ochrony prywatności. Główny problem koncentruje się na ryzyku związanym z przeniesieniem istotnych aplikacji lub danych z wewnątrz centrum obliczeniowego organizacji do centrum innej organizacji (tj. do chmury publicznej), która jest powszechnie dostępna do stosowania przez ogół społeczeństwa.

Istnieją trzy zasadnicze klasy chmur publicznych. Pierwsza klasa obejmuje te z usług, które są świadczone bez kosztów ponoszonych przez odbiorcę usług chmurowych, a jedynie są utrzymywane z reklam. Usługi wyszukiwania i poczty elektronicznej są dobrze znanymi przykładami. Takie usługi mogą być ograniczone do osobistego, niekomercyjnego użytku. Informacje zebrane przy rejestracji i podczas korzystania z usługi mogą być połączone z informacjami uzyskanymi z innych źródeł i wykorzystane do dostarczenia odbiorcy spersonalizowanych reklam. Może brakować również środków zabezpieczających, takich jak szyfrowana komunikacja z usługą. Druga klasa obejmuje chmury publiczne, których usługi są oparte na opłatach i nie zawierają reklam. Usługi w tej klasie mogą być podobne do tych z pierwszej klasy, ale mogą być oferowane po niskich kosztach dla odbiorcy usług chmurowych, ponieważ warunki świadczenia usług są nienegocjowane i mogą być modyfikowane jednostronnie według uznania dostawcy chmury. Zazwyczaj zapewniane są mechanizmy ochrony, które wykraczają poza te z pierwszej klasy i są konfigurowalne przez odbiorcę. Trzecia klasa obejmuje chmury publiczne, których usługi są oparte na opłatach i których warunki usług są negocjowane pomiędzy organizacją i dostawcą chmury. Podczas gdy usługi mogą być dostosowane do potrzeb organizacji, koszty są zazwyczaj zależne od stopnia odstępstwa od odpowiednich nienegocjowanych, opartych na opłatach usług oferowanych przez dostawcę chmury.

Obniżenie kosztów i zwiększenie wydajności są podstawowymi motywacjami do przejścia na chmurę publiczną, ale rezygnacja z odpowiedzialności za bezpieczeństwo nie powinna mieć miejsca. Ostatecznie, organizacja jest odpowiedzialna za wybór chmury publicznej oraz za bezpieczeństwo i prywatność zleconej usługi. Monitorowanie i rozwiązywanie pojawiających się kwestii bezpieczeństwa pozostaje w gestii organizacji, podobnie jak nadzór nad innymi ważnymi kwestiami, takimi jak wydajność i prywatność danych. Ponieważ przetwarzanie w chmurze niesie ze sobą nowe wyzwania związane z bezpieczeństwem, istotne jest, aby organizacja nadzorowała i zarządzała tym, w jaki sposób dostawca chmury zabezpiecza i utrzymuje środowisko obliczeniowe oraz zapewnia bezpieczeństwo danych.

3. USŁUGI CHMURY PUBLICZNEJ

Postrzeganie usług przetwarzania w chmurze może się znacznie różnić w zależności od organizacji, ze względu na nieodłączne różnice związane z celami, posiadanymi aktywami, zobowiązaniami prawnymi, ekspozycją na społeczeństwo, napotkanymi zagrożeniami i tolerancją na ryzyko. Na przykład, organizacja publiczna, która głównie obsługuje dane dotyczące poszczególnych obywateli kraju ma inne cele w zakresie ochrony prywatności i bezpieczeństwa niż organizacja publiczna, która takich celów nie realizuje. Podobnie, cele bezpieczeństwa organizacji publicznej, która przygotowuje i rozpowszechnia informacje do użytku publicznego, różnią się od tych, które dotyczą głównie informacji niejawnych na własny użytek wewnętrzny. Z perspektywy ryzyka określenie przez organizację stosowności korzystania z usług w chmurze nie jest możliwe bez zrozumienia kontekstu, w którym działa organizacja oraz konsekwencji wynikających z prawdopodobnych zagrożeń, przed którymi stoi. Zbiór celów bezpieczeństwa i ochrony prywatności organizacji jest zatem kluczowym czynnikiem przy podejmowaniu decyzji o outsourcingu usług informatycznych, a w szczególności przy podejmowaniu decyzji o przeniesieniu zasobów organizacyjnych do chmury publicznej oraz świadczeniu usług i rozwiązań usługowych konkretnego dostawcy. To, co sprawdza się w jednej organizacji, niekoniecznie musi sprawdzać się w innej. Ponadto, zastosowanie mają względy praktyczne - większość organizacji nie może sobie pozwolić finansowo na ochronę wszystkich zasobów obliczeniowych i aktywów w najwyższym możliwym stopniu i musi nadać priorytety dostępnym opcjom w oparciu o koszty, jak również krytyczność i newralgiczność. Rozważając potencjalne korzyści z publicznej chmury obliczeniowej, ważne jest, aby pamiętać o organizacyjnych celach związanych z bezpieczeństwem i ochroną prywatności i działać zgodnie z nimi. Ostatecznie, decyzja o przetwarzaniu w chmurze opiera się na analizie ryzyka związanego z określonymi opcjami kompromisowymi.[7]

[7] Proces przeprowadzania analizy ryzyka i zarządzania ryzykiem nie jest omawiany w niniejszej publikacji. Dodatkowe informacje dotyczące tych aspektów można znaleźć w publikacjach NSC 800-30, oraz NSC 800-37.

3.1. UMOWY O ŚWIADCZENIE USŁUG

Specyfikacje usług chmury publicznej i ustalenia dotyczące usług są zazwyczaj określane w umowach o świadczenie usług lub kontraktach na usługi. Umowa o świadczenie usług określa warunki dostępu i korzystania z usług oferowanych przez dostawcę chmury. Określa również okres świadczenia usługi, warunki zakończenia oraz dysponowanie danymi (np. okres przechowywania) po zakończeniu świadczenia usługi. Pełne warunki umowy o świadczenie usług w chmurze są zwykle określone w wielu dokumentach, które zwykle mogą obejmować Umowę gwarancji świadczenia usługi (*ang. Service Level Agreement - SLA*), politykę prywatności, politykę dopuszczalnego korzystania oraz warunki korzystania [Bra10]. SLA reprezentuje porozumienie pomiędzy odbiorcą chmury i dostawcą chmury dotyczące oczekiwanego poziomu jakości usługi, która ma być świadczona, oraz w przypadku, gdy dostawca nie dostarczy usługi na określonym poziomie, rekompensaty dostępnej dla odbiorcy chmury. Polityka prywatności dokumentuje praktyki przetwarzania informacji oraz sposób, w jaki informacje dotyczące odbiorcy usług chmurowych są gromadzone, wykorzystywane i zarządzane przez dostawcę usługi w chmurze. Polityka dopuszczalnego korzystania określa zakazane zachowania odbiorców usługi w chmurze. Warunki korzystania obejmują inne ważne szczegóły, takie jak licencjonowanie usług, ograniczenia odpowiedzialności oraz modyfikacje warunków umowy. Ryzyko związane z prywatnością i bezpieczeństwem zależy w dużym stopniu od warunków ustalonych w umowie o świadczenie usług.

Funkcjonują dwa rodzaje umów o świadczenie usług: predefiniowane umowy nienegocjowane oraz umowy negocjowane [Bra10, UCG10]. Umowy nienegocjowane są podstawą w wielu aspektach ekonomii skalowalności, z której korzysta publiczna chmura obliczeniowa. Warunki świadczenia usług są narzucane całkowicie przez dostawcę chmury. Zazwyczaj nie są one sformułowane z uwzględnieniem wymogów dotyczących ochrony prywatności i bezpieczeństwa [CIO10a]. Ponadto, w przypadku niektórych ofert dostawca może dokonywać modyfikacji warunków usługi jednostronnie (np. poprzez zamieszczenie zaktualizowanej wersji online) bez bezpośredniego powiadomienia odbiorcy chmury [Bra10].

Negocjowane umowy o świadczenie usług są bardziej zbliżone do tradycyjnych umów outsourcingowych na usługi informatyczne. Mogą być zawierane w celu rozwiązania problemów organizacji związanych z polityką bezpieczeństwa i prywatności, procedurami i zabezpieczeniami technicznymi, takimi jak rekrutacja pracowników, prawa własności danych i prawa do ich wycofania, powiadamianie o naruszeniach, izolacja aplikacji dzierżawionych, szyfrowanie i segregacja danych, śledzenie i raportowanie skuteczności usług, zgodność z przepisami i regulacjami oraz stosowanie zatwierdzonych produktów spełniających normy krajowe lub międzynarodowe (np. Federal Information Processing Standard 140-2 dla modułów kryptograficznych).

Krytyczne dane i aplikacje mogą wymagać od organizacji zawarcia negocjowanej umowy o świadczenie usług [Wall0]. Ponieważ punkty negocjacyjne mogą znacząco zakłócić i negatywnie wpłynąć na skalę korzyści, które nienegocjowana umowa o świadczenie usług wnosi do publicznego przetwarzania w chmurze, negocjowana umowa o świadczenie usług jest zazwyczaj mniej efektywna kosztowo. Wynik negocjacji jest również zależny od wielkości organizacji i wpływu, jaki może ona wywierać. Niezależnie od rodzaju umowy o świadczenie usług, zalecane jest uzyskanie odpowiedniej porady prawnej i technicznej w celu zapewnienia, że warunki usługi adekwatnie spełniają potrzeby organizacji.

3.2. BEZPIECZEŃSTWO I OCHRONA PRYWATNOŚCI - PLUSY

Podczas gdy jedną z największych przeszkód stojących przed publiczną chmurą obliczeniową jest bezpieczeństwo, paradygmat chmury obliczeniowej zapewnia możliwości innowacji w dostarczaniu usług bezpieczeństwa, które mają perspektywę poprawy ogólnego bezpieczeństwa niektórych organizacji. Największymi beneficjentami będą prawdopodobnie mniejsze organizacje, które mają ograniczoną liczbę administratorów technologii informatycznych i pracowników zajmujących się bezpieczeństwem, a dzięki przejściu do chmury publicznej mogą uzyskać określoną skalę korzyści dostępną dla większych organizacji z dużymi centrami danych.

Poprawa bezpieczeństwa ma również wpływ na prywatność. Oznacza to, że skuteczna ochrona prywatności może istnieć tylko na solidnych podstawach bezpieczeństwa

informacji. Jednakże prywatność, podobnie jak bezpieczeństwo, ma szerokie implikacje organizacyjne, operacyjne i techniczne. Pewne aspekty prywatności są ściśle związane z celami poufności, integralności i dostępności w zakresie bezpieczeństwa, jednakże niektóre z nich nie są z nimi związane. Wiążą się one natomiast z ważnymi zasadami i względami związanymi z prywatnością, które są przedmiotem prawa, regulacji i wytycznych [CIO10b].

Potencjalne obszary usprawnień, w których organizacje mogą czerpać korzyści w zakresie bezpieczeństwa i ochrony prywatności z przejścia do środowiska chmury publicznej obejmują następujące elementy:

- **Specjalizacja pracowników.** Dostawcy usług w chmurze, podobnie jak inne organizacje dysponujące obiektami obliczeniowymi o dużej skali, mają możliwość specjalizacji personelu w zakresie bezpieczeństwa, ochrony prywatności i innych obszarów o wysokim stopniu zainteresowania i znaczeniu dla organizacji. Wzrost skali przetwarzania danych prowadzi do rozwoju specjalizacji, co z kolei pozwala pracownikom odpowiedzialnym za bezpieczeństwo zrezygnować z innych obowiązków i skoncentrować się wyłącznie na kwestiach bezpieczeństwa i ochrony prywatności. Dzięki rosnącej specjalizacji członkowie personelu mają możliwość zdobycia dogłębnego doświadczenia i przeszkolenia, podjęcia działań zaradczych oraz wprowadzenia usprawnień w zakresie bezpieczeństwa i ochrony prywatności w sposób łatwiejszy niż byłoby to możliwe przy bardziej zróżnicowanym zakresie obowiązków.
- **Moc platformy.** Struktura platform obliczeniowych w chmurze jest zazwyczaj bardziej jednolita niż struktura większości tradycyjnych centrów obliczeniowych. Większa jednolitość i jednorodność ułatwiają wzmacnianie platformy i umożliwiają lepszą automatyzację działań związanych z zarządzaniem bezpieczeństwem, takich jak zabezpieczanie konfiguracji, testowanie podatności, audyty bezpieczeństwa i poprawki bezpieczeństwa komponentów platformy. Działania zapewniające wiarygodność informacji i reagowanie na zagrożenia również zyskują na jednolitej, jednorodnej infrastrukturze chmury, podobnie jak działania związane z zarządzaniem systemem, takie jak zarządzanie usterkami, równoważenie

obciążenia i konserwacja systemu. Analogicznie, jednorodność infrastruktury wpływa korzystnie na zarządzanie zabezpieczeniami stosowanymi w celu ochrony prywatności. Z drugiej strony, homogeniczność oznacza, że pojedyncza usterka będzie przejawiała się w całej chmurze, potencjalnie wpływając na wszystkich dzierżawców i usługi. Wiele środowisk przetwarzania w chmurze spełnia standardy zgodności operacyjnej i certyfikacji w takich obszarach, jak opieka zdrowotna (np. Health Insurance Portability and Accountability Act - HIPAA), finanse (np. Payment Card Industry Data Security Standard (PCI DSS)), bezpieczeństwo (np. ISO 27001, Information Security Management Systems - Requirements), oraz audyt (np. Standards for Attestation Engagements - SSAE No. 16), i może uzyskać formalną certyfikację lub atestację od niezależnej strony trzeciej, aby zapewnić poziom wiarygodności w odniesieniu do uznanych i ogólnie przyjętych kryteriów.

- **Dostępność zasobów.** Skalowalność infrastruktury chmury obliczeniowej zapewnia większą dostępność. Redundancja i możliwości odzyskiwania danych po awarii są wbudowane w środowiska chmur obliczeniowych, a pojemność zasobów na żądanie może być wykorzystywana w celu zwiększenia odporności w obliczu zwiększonego zapotrzebowania na usługi lub rozproszonych ataków typu „odmowa świadczenia usługi" (*ang. denial of service – DoS)*, a także w celu szybszego odzyskiwania danych po poważnych incydentach. W przypadku wystąpienia incydentu istnieje również możliwość powstrzymywania ataków i łatwiejszego pozyskiwania informacji o zdarzeniach, z większą szczegółowością i mniejszym wpływem na działalność produkcyjną. Dostępność może również wzmocnić prywatność dzięki lepszym możliwościom dostępu do zapisów i ich korygowania przez osoby oraz gotowości zapisów do wykorzystania w razie potrzeby do celów, dla których są gromadzone [CIO10b]. W niektórych przypadkach taka odporność i wydajność mogą mieć jednak swoje minusy. Na przykład, nieudany rozproszony atak typu DoS może szybko pochłonąć duże ilości zasobów do ochrony przed atakiem, co może spowodować szkody finansowe dla organizacji, jeśli opłaty za podwyższone zużycie w takich okolicznościach zostaną utrzymane. Dostęp do ogromnych ilości niedrogiej pamięci masowej może również spowodować, że gromadzonych będzie

więcej informacji niż potrzeba lub informacje będą przechowywane dłużej niż to konieczne.

- **Backup i odzyskiwanie.** Polityki i procedury tworzenia kopii zapasowych i odzyskiwania danych dostawcy usługi w chmurze mogą być lepsze od tych, które stosuje organizacja i mogą być bardziej solidne. Dane utrzymywane w chmurze mogą być bardziej dostępne, szybsze do przywrócenia i bardziej niezawodne w wielu okolicznościach niż te utrzymywane w tradycyjnym centrum danych, a także spełniać wymagania dotyczące przechowywania kopii zapasowych poza siedzibą firmy i zachowania zgodności geograficznej. W takich warunkach, usługi w chmurze mogą również służyć, jako repozytorium zewnętrzne dla centrum danych organizacji, w miejsce bardziej tradycyjnego taśmowego przechowywania zewnętrznego [Kum08]. Jednakże, wydajność sieci w Internecie i ilość danych są czynnikami ograniczającymi, które mogą wpłynąć na odtworzenie.
- **Mobilne punkty końcowe.** Architektura rozwiązania chmurowego rozszerza się na klienta w punkcie końcowym usługi (ang. endpoint), który jest używany do uzyskiwania dostępu do hostowanych aplikacji. Klientów chmury mogą stanowić przeglądarki internetowe ogólnego przeznaczenia lub aplikacje o bardziej specjalnym zastosowaniu. Ponieważ główne zasoby obliczeniowe potrzebne aplikacjom opartym na chmurze są zazwyczaj przechowywane przez dostawcę chmury, klienci mogą być generalnie mniej obciążeni obliczeniowo i łatwo obsługiwani na laptopach, notebookach i netbookach, a także na urządzeniach zintegrowanych, takich jak smartfony i tablety, co korzystnie wpływa na produktywność coraz bardziej mobilnej siły roboczej.[8] Jednym zastrzeżeniem do tego punktu jest to, że urządzenia mobilne, szczególnie urządzenia zintegrowane, wymagają odpowiedniej konfiguracji i ochrony, aby przynosiły ogólne korzyści, co

[8] Chociaż nie jest to sama w sobie korzyść związana z bezpieczeństwem, ta pozycja wiąże się z następną wypunktowaną pozycją Koncentracja danych.

obejmuje ograniczenia dotyczące rodzaju danych przechowywanych na urządzeniu [Jan08].

- **Koncentracja danych.** Dane utrzymywane i przetwarzane w chmurze publicznej mogą stanowić mniejsze ryzyko dla organizacji zatrudniającej pracowników mobilnych niż dane rozproszone w terenie na komputerach przenośnych, urządzeniach zintegrowanych lub nośnikach wymiennych, gdzie rutynowo dochodzi do kradzieży i utraty danych. Nie oznacza to jednak, że nie istnieje ryzyko, które jest związane z koncentracją danych.[9] Wiele organizacji dokonało przejścia na obsługę dostępu do danych organizacyjnych z urządzeń mobilnych w celu poprawy zarządzania przepływem pracy i uzyskania innych korzyści w zakresie efektywności operacyjnej i produktywności. Starannie skonstruowane aplikacje mogą ograniczyć dostęp i usługi tylko do tych danych i zadań, które ściśle odpowiadają obowiązkom użytkownika, ograniczając w ten sposób narażenie danych w przypadku kompromitacji urządzenia.

3.3. BEZPIECZEŃSTWO I OCHRONA PRYWATNOŚCI – MINUSY

Poza wieloma potencjalnymi korzyściami związanymi z bezpieczeństwem i ochroną prywatności, publiczne przetwarzanie w chmurze niesie ze sobą również potencjalne obszary zagrożeń, w porównaniu ze środowiskami obliczeniowymi znajdującymi się w tradycyjnych centrach danych. Niektóre z bardziej fundamentalnych zagrożeń obejmują następujące kwestie:

- **Złożoność systemu.** Środowisko chmury publicznej jest wyjątkowo złożone w porównaniu z tradycyjnym centrum danych. Na chmurę publiczną składa się wiele komponentów, co stwarza dużą powierzchnię ataku. Poza komponentami do ogólnego przetwarzania, takimi jak wdrożone aplikacje, monitory maszyn wirtualnych, maszyny wirtualne gości, przechowywanie danych i wspierające oprogramowanie pośredniczące, istnieją również komponenty, z których składa się

[9] Omówienie związanych z tym zagrożeń znajduje się w następnym rozdziale.

płaszczyzna zarządzania, takie jak komponenty do samoobsługi, pomiaru zasobów, zarządzania kwotami, replikacji i odzyskiwania danych, monitorowania poziomu usług, zarządzania obciążeniem pracą i gwałtownego wzrostu wykorzystania zasobów chmury.[10]

Usługi w chmurze mogą być również realizowane poprzez zagnieżdżanie i warstwowanie z usługami od innych dostawców chmury. Komponenty zmieniają się w czasie wraz z aktualizacjami i ulepszeniami funkcji, co dodatkowo komplikuje te kwestie.

Bezpieczeństwo zależy nie tylko od poprawności i efektywności wielu komponentów, ale także od interakcji pomiędzy nimi. Pojawiają się wyzwania związane ze zrozumieniem i zabezpieczeniem interfejsów programowania aplikacji, które często są zastrzeżone dla dostawcy chmury. Liczba możliwych interakcji pomiędzy komponentami wzrasta, jako kwadrat liczby komponentów, co powoduje wzrost poziomu złożoności. Złożoność zazwyczaj jest odwrotnie proporcjonalna do bezpieczeństwa, z większą złożonością powodującą zwiększoną podatność na ataki [Avo00, Gee08, Sch00]. Spadek bezpieczeństwa zwiększa również zagrożenia dla prywatności związane z utratą lub nieuprawnionym dostępem, zniszczeniem, wykorzystaniem, modyfikacją lub ujawnieniem danych osobowych.

- **Współdzielone środowisko wielu dzierżawców.** Usługi chmury publicznej oferowane przez dostawców usług chmurowych mają jeden podstawowy problem - organizacje klienckie zazwyczaj współdzielą komponenty i zasoby z innymi odbiorcami usług chmurowych, którzy nie są im znani. Zamiast wykorzystywać jako zabezpieczenie fizyczną separację zasobów, chmura obliczeniowa kładzie większy nacisk na separację logiczną na wielu warstwach stosu aplikacji [Owa10]. Choć nie jest to unikalne dla chmury obliczeniowej, separacja logiczna jest nietrywialnym problemem, który jest nasilony przez skalę chmury obliczeniowej (np. [Bos11]). Atakujący może podawać się za odbiorcę usługi chmurowej, aby wykorzystać podatności z wewnątrz środowiska chmury, pokonać mechanizmy separacji

[10] Gwałtowny wzrost wykorzystania zasobów chmury (*ang. Cloud bursting*) polega na rozmieszczeniu i uruchomieniu aplikacji w chmurze oraz przekierowaniu do niej żądań w przypadku, gdy zasoby obliczeniowe w centrum danych organizacji ulegną wyczerpaniu.

i uzyskać nieautoryzowany dostęp. Dostęp do danych i zasobów organizacyjnych może również zostać nieumyślnie ujawniony innym odbiorcom lub zostać zablokowany uprawnionym odbiorcom poprzez błąd w konfiguracji lub oprogramowaniu [Opp03].

Zagrożenia dla infrastruktur sieciowych i obliczeniowych rosną z każdym rokiem i stają się coraz bardziej wyrafinowane. Konieczność współdzielenia infrastruktury z nieznanymi podmiotami zewnętrznymi może być poważną ułomnością niektórych aplikacji i wymaga wysokiego poziomu wiarygodności co do siły mechanizmów bezpieczeństwa zastosowanych do logicznej separacji.

- **Usługi internetowe.** Usługi chmury publicznej są dostarczane przez Internet, uwidaczniając interfejsy administracyjne wykorzystywane do samodzielnego obsługiwania i zarządzania kontem, jak również interfejsy nieadministracyjnie wykorzystywane do dostępu do wdrożonych usług.[11] Aplikacje i dane, do których wcześniej uzyskiwano dostęp z ograniczonego intranetu organizacji, ale przeniesione do chmury publicznej, muszą teraz stawić czoła zwiększonemu ryzyku związanemu z zagrożeniami sieciowymi, przed którymi wcześniej zabezpieczano się na obrzeżach intranetu organizacji oraz przed nowymi zagrożeniami, które są wymierzone w odsłonięte interfejsy. Problemem może być również wydajność i jakość usług dostarczanych przez Internet. Efekt jest w pewnym sensie analogiczny do włączenia punktów dostępu bezprzewodowego do intranetu organizacji na początku istnienia tej technologii, co wymusza dodatkowe zabezpieczenia dotyczące bezpiecznego użytkowania.

  Poleganie na zdalnym dostępie administracyjnym, jako sposobie zarządzania aktywami przez organizację, które są przechowywane w chmurze, również zwiększa ryzyko w porównaniu z tradycyjnym centrum danych, gdzie dostęp

[11] Opracowano szereg rozwiązań do łagodzenia zagrożeń pochodzących z Internetu, w tym specjalne publikacje NIST SP 800-119, Wytyczne dotyczące bezpiecznego wdrażania IPv6--http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf; SP 500-267, Profil dla IPv6 w rządzie USA, Wersja 1.0; http://www.antd.nist.gov/usgv6/usgv6-v1.pdf; i SP-800-77, Przewodnik po IPsec VPN--http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf. Wsparcie ze strony dostawcy chmury jest warunkiem wstępnym do wdrożenia tych zabezpieczeń, a jak słusznie wskazano w tych publikacjach, exploity mogą nadal występować z powodu wadliwego wdrożenia i problemów z konfiguracją.

administracyjny do platform może być ograniczony do bezpośrednich lub wewnętrznych połączeń (np. [Som11]). Podobnie, zdalny dostęp administracyjny do infrastruktury chmury, jeśli jest wykonywany przez dostawcę chmury, również stanowi problem. W połączeniu z poprzednimi dwoma aspektami, wysoce złożone, korzystające z wielu dzierżaw środowisko przetwarzania, którego usługi są skierowane do Internetu i dostępne publicznie, niewątpliwie stanowi potencjalnie atrakcyjną powierzchnię ataku, która musi być starannie zabezpieczona.

- **Utrata kontroli.** Chociaż zagrożenia bezpieczeństwa i prywatności w usługach chmur obliczeniowych są analogiczne do tych w tradycyjnych usługach nieopartych na chmurze, są one wzmocnione przez zewnętrzne zabezpieczenie zasobów organizacyjnych i potencjalnych przyczyn niewłaściwego zarządzania tymi zasobami. Przejście do chmury publicznej wymaga przeniesienia odpowiedzialności i zabezpieczenia na dostawcę chmury nad informacjami, a także komponentami systemu, które wcześniej były pod bezpośrednią kontrolą organizacji. Przejściu temu towarzyszy zwykle brak bezpośredniego punktu kontaktu z zarządzającymi operacjami oraz wpływu na decyzje podejmowane w zakresie środowiska obliczeniowego. Taka sytuacja uzależnia organizację od współpracy z dostawcą chmury w zakresie realizacji działań, które obejmują zakres odpowiedzialności obu stron, takich jak ciągły monitoring i reagowanie na incydenty. Zgodność z przepisami i regulacjami dotyczącymi ochrony danych to kolejny ważny obszar wspólnej odpowiedzialności, który wymaga koordynacji i współpracy z dostawcą chmury.

  Utrata kontroli zarówno nad fizycznymi jak i logicznymi aspektami systemu i danych zmniejsza zdolność organizacji do utrzymywania świadomości sytuacyjnej, określania alternatyw, ustalania priorytetów i wprowadzania zmian w zakresie bezpieczeństwa i ochrony prywatności, które są w najlepszym interesie organizacji. Ochrona prawna prywatności może być również naruszona, gdy informacje są przechowywane u zewnętrznego dostawcy usług [Cou09, Han06]. W takich warunkach utrzymanie wiarygodności może być trudniejsze, co niweluje niektóre z potencjalnych korzyści omówionych wcześniej.

Szczegółowa dyskusja na temat kwestii bezpieczeństwa i ochrony prywatności, które wynikają z tych podstawowych problemów, przedstawiona jest w następnym rozdziale.

Inne rodzaje usług w chmurze.

Istnieją inne rodzaje usług w chmurze powiązane z bezpieczeństwem i ochroną prywatności. Poza zapewnieniem platformy obliczeniowej lub alternatywy dla wewnętrznych aplikacji, usługi chmury publicznej, takie jak poniższe, mogą również koncentrować się na zwiększaniu bezpieczeństwa w innych środowiskach obliczeniowych:

- **Zorientowane na centra danych** (*ang. Data Center Oriented*). Usługi w chmurze mogą być wykorzystane do poprawy bezpieczeństwa centrów danych. Informacje o działaniach on-line zebrane od wielu użytkowników z różnych organizacji mogą pozwolić na lepsze monitorowanie zagrożeń. Na przykład, poczta elektroniczna może być przekierowywana do dostawcy chmury za pośrednictwem rekordów wymiany poczty (ang. mail exchange - MX), badana i analizowana zbiorczo z podobnymi działaniami z innych centrów danych w celu wykrycia rozległych kampanii spamu, phishingu i złośliwego oprogramowania oraz przeprowadzenia działań zaradczych (np. kwarantanny podejrzanych wiadomości i treści) w sposób bardziej kompleksowy, niż byłaby w stanie to zrobić pojedyncza organizacja. Badacze z powodzeniem zademonstrowali również architekturę systemu do dostarczania usług antywirusowych opartych na chmurze, jako alternatywy dla rozwiązań antywirusowych opartych na hoście [Obe08b].
- **Zorientowane na chmurę** (*ang. Cloud Oriented*). Usługi w chmurze mogą być również wykorzystywane do poprawy bezpieczeństwa innych środowisk chmury. Na przykład dostępne są produkty typu "odwrotne proxy (ang. reverse proxy), które umożliwiają swobodny dostęp do środowiska SaaS, a jednocześnie utrzymują dane przechowywane w tym środowisku w postaci zaszyfrowanej [Nav10]. Istnieją również usługi zarządzania tożsamością w chmurze, które mogą być wykorzystywane do rozszerzenia lub zastąpienia usługi katalogowej organizacji w celu identyfikacji i uwierzytelniania użytkowników w chmurze.

W każdym obszarze technologicznym oferowane funkcje mogą zostać wykorzystane do niewłaściwych lub nielegalnych działań. Chmura obliczeniowa nie jest tu wyjątkiem. Pojawiło się już kilka wartych odnotowania przypadków, które dają wyobrażenie o tym, czego można się spodziewać w przyszłości:

- **Botnety**. Pod wieloma względami botnety gromadzone i kontrolowane przez hakerów są wstępną formą chmury obliczeniowej [Mul10]. Obniżenie kosztów, dynamiczne udostępnianie, redundancja, bezpieczeństwo i wiele innych cech charakterystycznych dla chmury obliczeniowej mają tu zastosowanie. Botnety były wykorzystywane do rozsyłania spamu, pozyskiwania danych uwierzytelniających do logowania oraz przeprowadzania ataków iniekcyjnych na strony WWW [Mul10, Pro09]. Botnety mogą być wykorzystane do przeprowadzenia ataku odmowy usługi na infrastrukturę dostawcy chmury. Sytuacja, w której usługa w chmurze może zostać infiltrowana przez botnet miała już miejsce; w 2009 roku odkryto węzeł dowodzenia i kontroli działający z wnętrza chmury IaaS [Mcm09a, Whi09]. Spamerzy kupowali również usługi w chmurze bezpośrednio w celu przeprowadzenia kampanii phishingowej, wykorzystując techniki socjotechniczne do zainfekowania odbiorców złośliwym oprogramowaniem [Cra08, Kre08].
- **Mechanizm łamania** (*ang. Mechanism Cracking*). WiFi Protected Access (WPA) Cracker, usługa w chmurze przeznaczona rzekomo dla testerów penetracyjnych, jest przykładem wykorzystania zasobów chmury na żądanie do złamania szyfru kryptograficznego i ustalenia zaszyfrowanego hasła używanego do ochrony sieci bezprzewodowej. Dzięki tej usłudze zadanie, które na pojedynczym komputerze zajęłoby pięć dni, może zostać wykonane w ciągu zaledwie 20 minut na klastrze 400 maszyn wirtualnych [Rag09]. Ponieważ kryptografia jest szeroko wykorzystywana w uwierzytelnianiu, poufności i integralności danych oraz innych mechanizmach bezpieczeństwa, mechanizmy te stają się w efekcie mniej efektywne wraz z dostępnością usług chmurowych umożliwiających łamanie kluczy kryptograficznych. Możliwym celem są zarówno systemy oparte na chmurze, jak i tradycyjne. Chmura IaaS została prawdopodobnie wykorzystana do ataku na sieć gier online i przejęcia kont ponad 100 milionów użytkowników [Alp11]. Łamanie

CAPTCHA to kolejny obszar, w którym usługi w chmurze mogą być stosowane do omijania weryfikacji mającej na celu udaremnienie nadużywania usług internetowych przez zautomatyzowane oprogramowanie.

4. KLUCZOWE KWESTIE ZWIĄZANE Z BEZPIECZEŃSTWEM I OCHRONĄ PRYWATNOŚCI

Chociaż pojawienie się chmur obliczeniowych jest wydarzeniem stosunkowo niedawnym, spostrzeżenia na temat krytycznych aspektów bezpieczeństwa można czerpać z doświadczeń pierwszych użytkowników, a także badaczy analizujących i eksperymentujących z dostępnymi platformami dostawców usług w chmurze i powiązanymi technologiami. Poniższe sekcje wskazują na kwestie związane z ochroną prywatności i bezpieczeństwem, które uważane są za mające długoterminowe znaczenie dla publicznego przetwarzania w chmurze oraz, w wielu przypadkach, dla innych modeli usług przetwarzania w chmurze. Tam, gdzie to możliwe, przykłady wcześniej przedstawionych lub zidentyfikowanych problemów są zamieszczone w celu zilustrowania danego zagadnienia. Przykłady nie są wyczerpujące i mogą obejmować tylko pojedynczy aspekt szerszego zagadnienia. W przypadku wielu z tych kwestii, konkretne omawiane problemy zostały już rozwiązane. Niemniej jednak, szerszy problem w większości przypadków nadal istnieje i może potencjalnie pojawić się ponownie w inny sposób w różnych modelach usług. Istnieją również uwarunkowania związane z bezpieczeństwem i ochroną prywatności, które wynikają z outsourcingu technologii informacyjnych; zostały one omówione w następnym rozdziale i stanowią uzupełnienie poniższego materiału.

Ponieważ chmury obliczeniowe wyrosły z kombinacji technologii, w tym architektury zorientowanej na usługi, wirtualizacji, Web 2.0 oraz przetwarzania narzędziowego (*ang. utility computing*), wiele z powiązanych kwestii dotyczących ochrony prywatności i bezpieczeństwa może być postrzeganych jako znane problemy w nowym otoczeniu. Znaczenie ich połączonego efektu w tym otoczeniu nie powinno być jednak pomijane. Publiczna chmura obliczeniowa stanowi inspirującą zmianę paradygmatu od konwencjonalnych norm do otwartej, zdepersonalizowanej infrastruktury organizacyjnej – w *skrajnym przypadku, przenosząc aplikacje z infrastruktury jednej organizacji do infrastruktury innej organizacji, gdzie mogą również działać aplikacje potencjalnych przeciwników.*

4.1. ZARZĄDZANIE

Zarządzanie oznacza kontrolę i nadzór organizacji nad zasadami, procedurami i standardami rozwoju aplikacji i pozyskiwania usług informatycznych, a także nad projektowaniem, implementacją, testowaniem, użytkowaniem i monitorowaniem wdrożonych lub wykorzystywanych usług. Przy szerokiej dostępności usług chmury obliczeniowej, brak kontroli organizacyjnej nad pracownikami arbitralnie korzystającymi z takich usług może okazać się źródłem problemów. Chociaż chmura obliczeniowa upraszcza proces pozyskiwania platform, nie eliminuje konieczności zarządzania, a wręcz przeciwnie - potęguje tę potrzebę.

Zaletą chmury obliczeniowej jest możliwość ograniczenia inwestycji kapitałowych w zasoby obliczeniowe, a zamiast tego zaspokojenie potrzeb obliczeniowych poprzez wydatki operacyjne. Chmura obliczeniowa może obniżyć początkowy koszt wdrożenia nowych usług i skrócić czas potrzebny do uzyskania wymiernych korzyści z inwestycji (tj. przyspieszyć czas do uzyskania wartości), tym samym lepiej dopasowując wydatki do rzeczywistego wykorzystania.[12] Jednakże, normalne procesy i procedury stosowane przez organizację w celu pozyskania zasobów obliczeniowych, jako nakładów kapitałowych, mogą być łatwo pominięte przez pojedynczą osobę lub komórkę organizacyjną, a zamówienia ukryte w ramach codziennych wydatków operacyjnych. Jeśli takie działania nie są regulowane przez organizację, jej polityka i procedury dotyczące ochrony prywatności, bezpieczeństwa i nadzoru mogą zostać przeoczone, a organizacja narażona na ryzyko. Na przykład, mogą zostać wdrożone wrażliwe systemy, zignorowane regulacje prawne, szybko narosnąć opłaty do niedopuszczalnego poziomu, zasoby zostać wykorzystane do nieusankcjonowanych celów lub mogą wystąpić inne niepożądane skutki.

Badanie przeprowadzone z udziałem ponad dziewięciuset specjalistów technologii informacyjnych w Europie i Stanach Zjednoczonych wskazuje na silne obawy uczestników, że w części ich organizacji usługi przetwarzania w chmurze mogły zostać

[12] Wiele firm przedkłada wydatki operacyjne nad nakłady kapitałowe ze względów podatkowych i innych finansowych (np. możliwość lepszego zarządzania kosztem kapitału i odliczania wydatków operacyjnych w okresie rozliczeniowym, w którym zostały poniesione, zamiast amortyzowania nakładów kapitałowych w czasie).

wdrożone bez ich wiedzy [Pon10]. Kwestia ta jest nieco podobna do problemu z osobami zakładającymi nieautoryzowane punkty dostępu do sieci bezprzewodowej podłączone do infrastruktury organizacyjnej - bez odpowiedniego zarządzania, organizacyjna infrastruktura obliczeniowa może zostać przekształcona w rozległą, niemożliwą do opanowania kombinację niezabezpieczonych usług. Praktyki organizacyjne odnoszące się do polityk, procedur i standardów wykorzystywanych do rozwoju aplikacji i nabywania usług, a także projektowania, wdrażania, testowania, korzystania i monitorowania wdrożonych lub zaangażowanych usług, powinny być rozszerzone na środowiska przetwarzania w chmurze.

Korzystanie z usług w chmurze wymaga zwrócenia uwagi na role i obowiązki zaangażowane pomiędzy organizacją, a dostawcą chmury, szczególnie w odniesieniu do zarządzania ryzykiem i zapewnienia, że wymagania organizacyjne są spełnione. Zapewnienie bezpieczeństwa systemów i zarządzania ryzykiem jest wyzwaniem w każdym środowisku, a jeszcze większym w przypadku chmur obliczeniowych. Mechanizmy i narzędzia audytu powinny być wdrożone w celu określenia, w jaki sposób dane są przechowywane, chronione i wykorzystywane w celu walidacji usług i weryfikacji egzekwowania polityk. Powinien również istnieć program zarządzania ryzykiem, który jest wystarczająco elastyczny, aby poradzić sobie z ciągle ewoluującym i zmieniającym się środowiskiem ryzyka.

4.2. ZGODNOŚĆ

Zgodność (*ang. compliance*) odnosi się do odpowiedzialności organizacji za działanie w zgodzie z ustalonymi przepisami prawa, regulacjami, standardami i specyfikacjami. Różnego rodzaju przepisy i regulacje dotyczące bezpieczeństwa i ochrony prywatności istnieją w różnych krajach na poziomie krajowym, stanowym i lokalnym, co sprawia, że zgodność jest potencjalnie skomplikowaną kwestią związaną z chmurą obliczeniową. Na przykład, pod koniec 2010 roku Krajowa Konferencja Ustawodawców Stanowych poinformowała, że czterdzieści sześć stanów uchwaliło prawa regulujące ujawnianie naruszeń bezpieczeństwa danych osobowych, a co najmniej dwadzieścia dziewięć

stanów uchwaliło prawa regulujące usuwanie danych osobowych będących w posiadaniu firm i/lub rządu[13].

- **Przepisy prawne i regulacje.**[14] Z punktu widzenia amerykańskich agencji federalnych, główne problemy związane z bezpieczeństwem i zgodnością z ochroną prywatności zawarte są w ustawie Clinger-Cohen z 1996 r., okólniku Biura Zarządzania i Budżetu (OMB) nr A-130, w szczególności w załączniku III, ustawie o ochronie prywatności z 1974 r., ustawie o elektronicznej administracji z 2002 r. i towarzyszących jej wytycznych OMB oraz ustawie o zarządzaniu bezpieczeństwem informacji federalnych (FISMA) z 2002 r. Istotne znaczenie mają również ustawy Krajowej Administracji Archiwów i Rejestrów (NARA), w tym ustawa o rejestrach federalnych (44 U.S.C. rozdziały 21, 29, 31, 33) oraz przepisy NARA (tytuł 36 Kodeksu Przepisów Federalnych, rozdział XII, podrozdział B). Ustawa Clinger-Cohen przypisuje odpowiedzialność za wydajność, bezpieczeństwo i prywatność w systemach komputerowych w ramach rządu federalnego i ustanawia kompleksowe podejście dla agencji wykonawczych w celu poprawy nabywania i zarządzania ich zasobami informacyjnymi. W ramach obowiązków OMB wynikających z ustawy Clingera-Cohena wydano różne okólniki. Okólnik A-130 ustanawia politykę zarządzania federalnymi zasobami informacyjnymi, w tym wytyczne proceduralne i analityczne dotyczące wdrażania poszczególnych aspektów tej polityki. Załącznik III do A-130 wymaga zapewnienia odpowiedniego bezpieczeństwa wszystkich informacji agencji, które są gromadzone, przetwarzane, przekazywane, przechowywane lub rozpowszechniane w ogólnych systemach wsparcia i głównych aplikacjach.
  Ustawa o ochronie prywatności reguluje gromadzenie, utrzymywanie, wykorzystywanie i rozpowszechnianie informacji o osobach fizycznych, które są

[13] Więcej szczegółowych informacji można znaleźć na stronie Issues & Research on Telecommunications & Information Technology
http://www.ncsl.org/.

[14] Przywołane przepisy i regulacje odnoszą się do środowiska amerykańskiego i nie mają zastosowania na rynku polskim. Zostały podane jako przykład dla zainteresowanych, chcących poszerzyć swoją wiedzę.

przechowywane w systemach rejestrów przez agencje federalne i mogą być wyszukane na podstawie osobistego identyfikatora (np. nazwiska). Wymaga ona, aby każda agencja opublikowała w Rejestrze Federalnym zawiadomienie o swoich systemach rejestrów (tj. zawiadomienie o systemie rejestrów (SORN)) oraz aby umożliwiła osobom fizycznym składanie wniosków o dostęp do swoich rejestrów i informacji oraz ich korektę. Ustawa o elektronicznej administracji z 2002 r., między innymi, wymaga od agencji federalnych przeprowadzenia oceny wpływu na prywatność (PIA) w odniesieniu do wszystkich nowych lub znacznie zmienionych technologii, które gromadzą, przechowują lub rozpowszechniają informacje osobiste, oraz publicznego udostępnienia wyników. M-03-22, Wytyczne OMB w sprawie wdrażania przepisów ustawy o prywatności w administracji elektronicznej z 2002 r. (OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002), zawiera wskazówki dla agencji dotyczące przeprowadzania PIA. PIA jest ustrukturyzowanym przeglądem systemu informacyjnego w celu zidentyfikowania i złagodzenia zagrożeń dla prywatności, w tym zagrożeń dla poufności, na każdym etapie cyklu życia systemu. Może ona również służyć, jako narzędzie dla osób pracujących nad programem lub mających dostęp do systemu w celu zrozumienia, jak najlepiej zintegrować ochronę prywatności podczas pracy z PII.

FISMA wymaga od agencji federalnych odpowiedniej ochrony ich informacji i systemów informacyjnych przed nieuprawnionym dostępem, wykorzystaniem, ujawnieniem, zakłóceniem, modyfikacją lub zniszczeniem [HR2458]. Mandat ten obejmuje ochronę systemów informacyjnych używanych lub obsługiwanych przez agencję lub przez kontrahenta agencji lub inną organizację w imieniu agencji. Oznacza to, że każdy zewnętrzny dostawca korzystający z informacji federalnych lub obsługujący systemy informacyjne w imieniu rządu federalnego musi spełniać te same wymogi bezpieczeństwa, co źródłowa agencja federalna. Wymogi bezpieczeństwa dotyczą również zewnętrznych podsystemów przechowujących, przetwarzających lub przekazujących informacje federalne oraz wszelkich usług świadczonych przez podsystem lub z nim związanych.

Zgodnie z Federal Records Act i regulacjami NARA, agencje są odpowiedzialne za efektywne zarządzanie dokumentacją federalną w całym cyklu jej życia, w tym dokumentacją w elektronicznych systemach informacyjnych i w środowiskach kontraktowych. Jeśli wykonawca posiada dokumentację federalną, musi nią zarządzać zgodnie ze wszystkimi obowiązującymi przepisami i regulacjami dotyczącymi zarządzania dokumentacją. Zarządzanie dokumentacją obejmuje bezpieczne przechowywanie, odzyskiwanie i właściwe dysponowanie, w tym przekazywanie trwale wartościowych zapisów do NARA w akceptowalnym formacie [Fer10].

Inne wymagania rządowe i stowarzyszenia branżowe, takie jak Health Insurance Portability and Accountability Act (HIPAA) oraz Payment Card Industry Data Security Standard (PCI DSS), mogą mieć zastosowanie do konkretnej organizacji. Na przykład, Veterans Health Administration podlega przepisom HIPAA dla prywatnych i publicznych zakładów opieki zdrowotnej, które dotyczą zarówno pracowników, jak i wykonawców [DVA]. HIPAA wymaga zarówno technicznych, jak i fizycznych zabezpieczeń do kontroli dostępu do chronionych informacji zdrowotnych, co może stwarzać problemy ze zgodnością dla niektórych dostawców usług w chmurze.

Dostawcy usług w chmurze stają się coraz bardziej wrażliwi na kwestie prawne i regulacyjne, i mogą być skłonni zobowiązać się do przechowywania i przetwarzania danych w określonych jurysdykcjach oraz stosować wymagane zabezpieczenia w zakresie bezpieczeństwa i prywatności. Nie wiadomo jednak, w jakim stopniu będą oni akceptować odpowiedzialność w swoich umowach o świadczenie usług, za narażenie treści znajdujących się pod ich kontrolą. Mimo to, organizacje są ostatecznie odpowiedzialne za bezpieczeństwo i prywatność danych przechowywanych przez dostawcę usług w chmurze w ich imieniu.

- **Lokalizacja danych.** Jednym z najczęstszych problemów związanych ze zgodnością z przepisami, przed jakimi staje organizacja, jest lokalizacja danych [Bin09, Kan09, Ove10]. Korzystanie z własnego centrum obliczeniowego pozwala organizacji na ustrukturyzowanie swojego środowiska obliczeniowego i szczegółową wiedzę na temat tego, gdzie dane są przechowywane i jakie zabezpieczenia są stosowane

w celu ochrony danych. W przeciwieństwie do tego, cechą wielu usług chmury obliczeniowej jest to, że dane są przechowywane redundantnie w wielu fizycznych lokalizacjach, a szczegółowe informacje o lokalizacji danych organizacji są niedostępne lub nieujawnione odbiorcy usługi. Taka sytuacja utrudnia ustalenie, czy istnieją wystarczające zabezpieczenia oraz czy spełnione są wymogi zgodności z prawem i regulacjami. Na przykład, przepisy NARA (tj. 36 CFR 1234) zawierają wymagania dotyczące obiektów do przechowywania dokumentacji rządowej i określają minimalną wysokość nad terenem zalewowym i odległość od niego. Audyty zewnętrzne i certyfikaty bezpieczeństwa mogą do pewnego stopnia złagodzić ten problem, ale nie są panaceum [Mag10].

W przypadku, gdy informacje są przekazywane poza granice kraju, obowiązujące systemy prawne, ochrony prywatności i regulacyjne mogą być niejednoznaczne i budzić różnorodne obawy (np. [CBC04, Wei11]). W związku z tym, ograniczenia dotyczące transgranicznego przepływu danych wrażliwych, jak również wymagania dotyczące ochrony danych, stały się przedmiotem krajowych i regionalnych praw i regulacji w zakresie prywatności i bezpieczeństwa [Eis05].

Główne obawy dotyczące zgodności z przepisami w przypadku transgranicznych przepływów danych obejmują rozstrzygnięcie, czy prawo obowiązujące w jurysdykcji, w której dane zostały zgromadzone, zezwala na przepływ danych, czy prawo to ma nadal zastosowanie do danych po ich przekazaniu oraz czy prawo obowiązujące w miejscu przeznaczenia nie stwarza dodatkowego ryzyka lub zapewnia dodatkowe korzyści [Eis05]. Często stosuje się zabezpieczenia techniczne, fizyczne i administracyjne, takie jak kontrola dostępu. Na przykład, europejskie przepisy o ochronie danych mogą nakładać dodatkowe obowiązki w zakresie obsługi i przetwarzania danych przekazywanych do USA [DoC00]. Te obawy mogą być złagodzone, jeżeli dostawca usługi w chmurze posiada wiarygodne środki do zapewnienia, że dane organizacji są przechowywane i przetwarzane tylko w określonych jurysdykcjach.

- **Rozpoznawanie dowodów elektronicznych.** Elektroniczne odkrywanie obejmuje identyfikację, gromadzenie, przetwarzanie, analizę i produkcję elektronicznie przechowywanych informacji (*ang. Electronically Stored Information - ESI*) w fazie

ujawniania informacji w postępowaniu sądowym [Daw05]. Organizacje mają również inne motywacje i obowiązki związane z przechowywaniem i wytwarzaniem dokumentów elektronicznych, takie jak zgodność z wymaganiami audytu i przepisami prawnymi, a w przypadku organizacji rządowych, zgodność z wymaganiami ustawy o wolności informacji (*ang. Freedom of Information Act - FOIA*). ESI obejmuje nie tylko pocztę elektroniczną, załączniki i inne obiekty danych przechowywane w systemie informacyjnym lub na nośniku, ale także wszelkie powiązane metadane, takie jak daty utworzenia lub modyfikacji obiektu oraz niewyodrębnioną zawartość pliku (tj. dane, które nie są wyraźnie wyświetlane dla konsumentów).

Możliwości i procesy dostawcy chmury, takie jak forma, w jakiej dane są utrzymywane oraz dostępne narzędzia związane z elektronicznym odkrywaniem, wpływają na zdolność organizacji do wypełniania swoich obowiązków w sposób efektywny kosztowo, terminowy i zgodny z przepisami [Mcd10]. Na przykład możliwości archiwizacyjne dostawcy usługi w chmurze mogą nie zachowywać oryginalnych metadanych zgodnie z oczekiwaniami, powodując fragmentację (tj. celowe, lekkomyślne lub niedbałe zniszczenie, utratę, istotną zmianę lub blokadę dowodów, które są istotne dla postępowania sądowego), co może negatywnie wpłynąć na postępowanie sądowe. Możliwości i procesy elektronicznego odkrywania dostawcy chmury nie mogą naruszać prywatności lub bezpieczeństwa danych i aplikacji organizacji podczas spełniania obowiązków związanych z odkrywaniem innych odbiorców chmury i vice versa.

4.3. ZAUFANIE

W paradygmacie chmury obliczeniowej organizacja zrzeka się bezpośredniej kontroli nad wieloma aspektami bezpieczeństwa i ochrony prywatności, a czyniąc to, powierza wysoki poziom zaufania dostawcy chmury. Jednocześnie organizacje są odpowiedzialne za ochronę informacji i systemów informacyjnych współmiernie do ryzyka i skali szkód wynikających z nieuprawnionego dostępu, wykorzystania, ujawnienia, zakłócenia, modyfikacji lub zniszczenia, niezależnie od tego, czy informacje są gromadzone lub przechowywane przez organizację lub w jej imieniu; lub czy systemy

informacyjne są wykorzystywane lub obsługiwane przez organizację lub przez wykonawcę organizacji lub inną organizację w imieniu organizacji [HR2458].

- **Dostęp osób nieupoważnionych.** Dane przetwarzane lub przechowywane poza fizycznymi ramami organizacji, jej zaporą sieciową i innymi środkami bezpieczeństwa niosą ze sobą nieodłączny poziom ryzyka. Zagrożenie bezpieczeństwa związane z wykorzystaniem informacji poufnych jest dobrze znanym problemem dla większości organizacji i, niezależnie od nazwy, ma zastosowanie również do usług chmurowych świadczonych na zasadzie outsourcingu [Ash10, Cap09, Kow08]. Zagrożenia wewnętrzne nie ograniczają się do tych stwarzanych przez obecnych lub byłych pracowników i odnoszą się też do wykonawców, podmiotów powiązanych z organizacją oraz innych stron, które uzyskały dostęp do sieci, systemów i danych organizacji w celu przeprowadzenia lub umożliwienia działalności operacyjnej. Incydenty mogą obejmować różnego rodzaju oszustwa, sabotaż zasobów informacyjnych oraz kradzież poufnych informacji. Incydenty mogą być również spowodowane nieumyślnie - na przykład pracownik banku rzekomo wysłał poufne informacje o kliencie na niewłaściwe konto pocztowe Google [Zet09b].
  Przeniesienie danych i aplikacji do środowiska chmur obliczeniowych obsługiwanych przez dostawcę chmury rozszerza krąg osób wtajemniczonych nie tylko na pracowników i podwykonawców dostawcy chmury, ale także potencjalnie na innych klientów korzystających z usługi, zwiększając tym samym ryzyko. Przykładowo, zademonstrowano atak typu DoS przeprowadzony przez złośliwego testera na znaną chmurę IaaS [Mee09, Sla09]. Atak polegał na tym, że odbiorca chmury utworzył początkowo 20 kont i uruchomił dla każdego z nich wirtualne maszyny, a następnie wykorzystał te konta do utworzenia kolejnych 20 kont i maszyn w sposób iteracyjny, wykładniczo zwiększając i zużywając zasoby ponad ustalone limity.
- **Własność danych.** Prawa własności organizacji do danych muszą być ściśle określone w umowie o świadczenie usług, aby zapewnić podstawę dla zaufania i prywatności danych. Ciągłe kontrowersje dotyczące prywatności i praw własności

danych użytkowników sieci społecznościowych ilustrują wpływ, jaki niejednoznaczne warunki mogą mieć na zaangażowane strony (np. [Goo10, Rap09]). W najlepszym przypadku umowa powinna wyraźnie stwierdzać, że organizacja zachowuje wyłączną własność wszystkich swoich danych; dostawca usługi w chmurze nie nabywa żadnych praw lub licencji poprzez umowę, w tym praw lub licencji własności intelektualnej do wykorzystywania danych organizacji do własnych celów; oraz, że dostawca usługi w chmurze nie nabywa i nie może rościć sobie żadnych praw do danych z związku z zapewnieniem bezpieczeństwa [Mcd10]. Aby te postanowienia działały zgodnie z przeznaczeniem, warunki własności danych nie mogą podlegać jednostronnej zmianie przez dostawcę usługi w chmurze.

- **Usługi zagregowane. U**sługi w chmurze mogą być komponowane poprzez zagnieżdżanie i warstwowanie z innymi usługami w chmurze. Na przykład, publiczny dostawca SaaS może budować swoje usługi na usługach chmury PaaS lub IaaS. Poziom dostępności chmury SaaS zależałby wtedy od dostępności tych usług. Jeśli procentowa dostępność usługi wsparcia spada, proporcjonalnie spada ogólna dostępność. Usługi w chmurze, które wykorzystują zewnętrznych dostawców usług w chmurze do zlecania na zewnątrz lub podwykonawstwa niektórych swoich usług powinny wzbudzać obawy, włączając w to zakres kontroli nad stroną trzecią, związane z tym obowiązki (np. ustalenia dotyczące polityki i licencjonowania) oraz środki zaradcze i regresy dostępne w przypadku wystąpienia jakichkolwiek problemów. Dostawcy chmury publicznej, którzy hostują aplikacje lub usługi innych stron mogą angażować inne zakresy zabezpieczeń, ale poprzez przejrzyste mechanizmy uwierzytelniania są postrzegani przez odbiorcę jako dostawcy chmury. Zaufanie często nie jest przejściowe, co wymaga, aby ustalenia dotyczące stron trzecich zostały ujawnione przed zawarciem umowy z dostawcą usługi w chmurze oraz aby warunki tych ustaleń były utrzymywane przez cały okres obowiązywania umowy lub do czasu, gdy można odpowiednio powiadomić o wszelkich przewidywanych zmianach.

Gwarancje odpowiedzialności i wydajności mogą stać się istotnym problemem w przypadku złożonych usług w chmurze. Na przykład, usługa sieci społecznościowej wykorzystująca pamięć masową klientów została zamknięta po utracie dostępu do znacznej ilości danych swoich 20.000 klientów. Ponieważ opierała się na innym dostawcy chmury do hostowania danych historycznych, a na jeszcze innym dostawcy chmury do hostowania swojej nowo uruchomionej aplikacji i bazy danych, bezpośrednia odpowiedzialność za przyczynę awarii była niejasna i nigdy nie została rozwiązana [Bro08].

- **Przejrzystość.** Ciągłe monitorowanie bezpieczeństwa informacji wymaga bieżącego utrzymywania znajomości środków bezpieczeństwa, podatności i zagrożeń w celu wspierania decyzji związanych z zarządzaniem ryzykiem [Dem10]. Zbieranie i analizowanie dostępnych danych o stanie systemu powinno być wykonywane regularnie i tak często, jak jest to niezbędne organizacji do zarządzania ryzykiem związanym z bezpieczeństwem i ochroną prywatności, odpowiednio dla każdego poziomu organizacji zaangażowanego w podejmowanie decyzji. Przejście na usługi chmury publicznej wiąże się z przeniesieniem odpowiedzialności na dostawcę chmury za zabezpieczenie części systemu, w którym przetwarzane są dane i aplikacje organizacji. W celu wypełnienia obowiązków ciągłego monitorowania organizacja jest zależna od dostawcy chmury, którego współpraca jest niezbędna, ponieważ aspekty środowiska przetwarzania znajdują się pod pełną kontrolą dostawcy chmury.
  Wiedza o stosowanych przez dostawcę chmury środkach bezpieczeństwa jest również potrzebna organizacji do sprawnego zarządzania ryzykiem. Na przykład, proces identyfikacji podatności powinien obejmować analizę właściwości zabezpieczeń systemu oraz środków bezpieczeństwa stosowanych do ochrony środowiska chmury [Sto02]. Dostawcy chmury mogą być jednak niechętni do podawania szczegółów dotyczących ich zabezpieczeń i ochrony prywatności oraz ich stanu, ponieważ takie informacje są często uważane za informacje prawnie chronione i mogą być w rezultacie wykorzystane do opracowania dróg ataku. Ponadto, szczegółowe monitorowanie przez odbiorcę chmury warstwy sieciowej i systemowej zazwyczaj nie jest zawarte w większości umów o świadczenie usług,

ograniczając bezpośrednią widoczność i sposób monitorowania operacji do audytu (np. [Bro09, Dig08, Met09]). Podczas gdy narzędzia powiadamiania i pulpity nawigacyjne oparte na sieci Web są zazwyczaj udostępniane odbiorcom w celu monitorowania statusu, może im brakować wystarczającej szczegółowości i sami mogą doświadczyć zakłóceń podczas niedostępności systemu [Goo09a, Ker11, Per11].

Przejrzystość w sposobie działania dostawcy chmury, w tym świadczenia usług zagregowanych, jest istotnym składnikiem efektywnego nadzoru bezpieczeństwa systemu i ochrony prywatności przez organizację. W celu zapewnienia, że polityka i procedury są egzekwowane w całym cyklu życia systemu, umowy dotyczące usług powinny zawierać pewne rozwiązania, dzięki którym organizacja może uzyskać wgląd w mechanizmy bezpieczeństwa i procesy stosowane przez dostawcę chmury oraz ich wydajność w czasie. Na przykład, umowa o świadczenie usług może zawierać prawo do audytu zabezpieczeń za pośrednictwem strony trzeciej, jako sposób na zatwierdzenie parametrów zabezpieczeń, które nie są w inny sposób dostępne lub możliwe do oceny przez odbiorcę. Idealnie byłoby, gdyby odbiorca usług chmurowych miał kontrolę nad aspektami dotyczącymi środków przejrzystości, aby dostosować je do swoich potrzeb, takich jak próg alarmów i powiadomień oraz poziom szczegółowości i harmonogram raportów.

- **Dane pomocnicze.** Pomimo tego, że uwaga w chmurze obliczeniowej skupia się głównie na ochronie danych aplikacyjnych, dostawcy chmur przechowują również istotne szczegóły dotyczące kont odbiorców chmury, które mogą zostać skompromitowane i wykorzystane w późniejszych atakach. Informacje o płatnościach są jednym z przykładów; inne, bardziej subtelne rodzaje informacji, również mogą być wykorzystane. Na przykład, baza danych z informacjami kontaktowymi wykradziona od dostawcy chmury SaaS, poprzez ukierunkowany atak phishingowy na jednego z jego pracowników, została z kolei wykorzystana do przeprowadzenia udanych ukierunkowanych ataków pocztą elektroniczną na odbiorców usługi w chmurze [Kre07, Mcm07]. Incydent ten obrazuje konieczność, aby dostawcy usług w chmurze chronili i niezwłocznie zgłaszali naruszenia bezpieczeństwa występujące nie tylko w danych, które dostawca usługi w chmurze

przechowuje na potrzeby swoich klientów, ale również w danych, które przechowuje na temat swoich konsumentów, niezależnie od tego, czy dane są przechowywane w infrastrukturze chmury, czy też niezależnie od niej. Inne rodzaje danych pomocniczych, które istnieją, obejmują informacje, które dostawca usługi w chmurze gromadzi lub wytwarza na temat aktywności związanej z klientem w chmurze. Obejmują one dane gromadzone w celu mierzenia i naliczania opłat za wykorzystanie zasobów, dzienniki i ścieżki audytu oraz inne tego rodzaju metadane, które są generowane i gromadzone w środowisku chmury. W przeciwieństwie do danych organizacyjnych, dostawca usługi w chmurze może być bardziej skłonny do roszczenia sobie prawa własności do danych operacyjnych i innych rodzajów metadanych, które gromadzi. Takie dane, jeżeli zostaną sprzedane, udostępnione lub wyciekną do strony trzeciej, stanowią jednak potencjalne zagrożenie dla prywatności organizacji, ponieważ dane te mogą być wykorzystane do określenia statusu i perspektyw inicjatywy organizacji (np. poziom aktywności lub przewidywany rozwój). Kilka punktów, nad których wyjaśnieniem należy się zastanowić w umowie o świadczenie usług to rodzaje metadanych gromadzonych przez dostawcę usługi w chmurze, ochrona zapewniona metadanym oraz prawa organizacji w odniesieniu do metadanych, w tym własność, rezygnacja z gromadzenia lub dystrybucji oraz dozwolone wykorzystanie.

- **Zarządzanie ryzykiem.** W przypadku usług opartych na chmurze, niektóre podsystemy lub komponenty podsystemu znajdują się poza bezpośrednią kontrolą organizacji klienta. Wiele organizacji czuje się bardziej komfortowo podejmując ryzyko, gdy ma większą kontrolę nad procesami i wykorzystywanym sprzętem. Jako minimum, wysoki stopień zabezpieczeń zapewnia możliwość rozważenia alternatyw, ustalenia priorytetów i zdecydowanego działania w najlepszym interesie organizacji w przypadku wystąpienia incydentu. Zarządzanie ryzykiem jest procesem identyfikacji i oceny ryzyka związanego z funkcjonowaniem systemu informacyjnego dla działalności organizacji, jej aktywów lub osób oraz podejmowania niezbędnych kroków w celu jego redukcji do akceptowalnego poziomu [Sto02]. Proces ten obejmuje przeprowadzenie oceny ryzyka, wdrożenie

strategii ograniczania ryzyka oraz zastosowanie technik i procedur ciągłego monitorowania stanu bezpieczeństwa systemu informacyjnego.[15] Systemy oparte na chmurze publicznej, podobnie jak tradycyjne systemy informacyjne, wymagają zarządzania ryzykiem w całym cyklu życia systemu.

Ocena i zarządzanie ryzykiem w systemach, które korzystają z usług w chmurze może być prawdziwym wyzwaniem. FISMA i polityka OMB wymagają od zewnętrznych dostawców, którzy zajmują się informacjami rządowymi lub obsługują systemy informacyjne w imieniu rządu, aby spełniali te same wymagania bezpieczeństwa, co organizacje rządowe [JTF10]. W maksymalnym możliwym zakresie, organizacje powinny zapewnić, że środki ochrony prywatności i bezpieczeństwa są prawidłowo wdrożone, działają zgodnie z przeznaczeniem i spełniają stawiane im wymagania. Organizacje powinny zrozumieć środki ochrony prywatności i bezpieczeństwa usługi w chmurze, wprowadzić odpowiednie ustalenia w umowie o świadczenie usług, dokonując wszelkich potrzebnych dostosowań oraz monitorować zgodność zabezpieczeń usług z postanowieniami umowy.

Ustanowienie poziomu zaufania do usługi w chmurze zależy od stopnia kontroli, jaki organizacja jest w stanie wywrzeć na dostawcę, aby zapewnił środki bezpieczeństwa niezbędne do ochrony danych i aplikacji organizacji, a także od dostarczonych dowodów na skuteczność tych zabezpieczeń [JTF10]. Jednak weryfikacja prawidłowego funkcjonowania podsystemu i skuteczności środków bezpieczeństwa w tak szerokim zakresie, jak w przypadku systemu organizacyjnego, może być w niektórych przypadkach niewykonalna, a do ustalenia poziomu zaufania można wykorzystać inne środki (np. audyty stron trzecich). Ostatecznie, jeżeli poziom zaufania do usługi spadnie poniżej oczekiwań, a organizacja nie jest w stanie zastosować zabezpieczeń kompensacyjnych, musi albo odrzucić usługę, albo zaakceptować większy stopień ryzyka.

[15] Bardziej szczegółowe informacje na temat zarządzania ryzykiem można znaleźć w dokumencie NSC 800-37.

4.4. ARCHITEKTURA

Architektura oprogramowania i sprzętu wykorzystywanego do świadczenia usług w chmurze może się znacznie różnić wśród dostawców chmury publicznej w odniesieniu do konkretnego modelu usług. Fizyczna lokalizacja infrastruktury jest określana przez dostawcę chmury, podobnie jak koncepcja i implementacja niezawodności, łączenia zasobów, skalowalności i innej logiki niezbędnej w ramach wsparcia. Aplikacje są budowane w oparciu o interfejsy programistyczne usług dostępnych przez Internet, które zazwyczaj obejmują wiele komponentów chmury komunikujących się ze sobą za pomocą interfejsów programowania aplikacji. Maszyny wirtualne zazwyczaj służą jako abstrakcyjna jednostka wdrożenia dla chmur IaaS i są luźno powiązane z architekturą pamięci masowej w chmurze. Dostawcy chmur mogą również korzystać z innych abstrakcji obliczeniowych zastępujących technologię maszyn wirtualnych w celu świadczenia usług w innych modelach usług.

Uzupełnieniem rozwiązania po stronie serwera są aplikacje oparte na chmurze, które wymagają zastosowania warstwy klienta do inicjowania i uzyskiwania usług. Chociaż przeglądarki internetowe często służą jako aplikacje klienckie, dostępne są również inne rozwiązania. Ponadto, musi istnieć odpowiednia i bezpieczna infrastruktura komunikacji sieciowej. Wiele z uproszczonych interfejsów i abstrakcji usług na poziomie klienta, serwera i sieci nie jest zgodnych z nieodłączną złożonością, która wpływa na bezpieczeństwo i ochronę prywatności. Dlatego ważne jest, aby zrozumieć technologie, które dostawca chmury wykorzystuje do świadczenia usług oraz wpływ, jaki zastosowane zabezpieczenia techniczne mają na bezpieczeństwo i prywatność w systemie w całym jego cyklu życia. Posiadając takie informacje, architektura systemu leżącego u podstaw chmury może zostać zdekomponowana i przyporządkowana do modelu zabezpieczeń i ochrony prywatności, które mogą być wykorzystane do oceny i zarządzania ryzykiem.

Powierzchnia ataku. Hiperwizor lub monitor maszyn wirtualnych jest dodatkową warstwą oprogramowania pomiędzy systemem operacyjnym, a platformą sprzętową, która jest używana do obsługi wielodostępowych maszyn wirtualnych i jest wspólna dla chmur IaaS. Oprócz zwirtualizowanych zasobów, hiperwizor zwykle obsługuje inne

interfejsy programowania aplikacji do wykonywania operacji administracyjnych, takich jak uruchamianie, migracja i kończenie operacji na maszynach wirtualnych.
W porównaniu z tradycyjną, niezwirtualizowaną implementacją, dodanie hiperwizora powoduje zwiększenie powierzchni ataku. Oznacza to, że istnieją dodatkowe metody (np. interfejsy programowania aplikacji), kanały (np. gniazda) i elementy danych (np. łańcuchy wejściowe), które napastnik może wykorzystać do wyrządzenia szkód w systemie.
Złożoność środowisk maszyn wirtualnych może być również wyzwaniem większym niż w przypadku ich tradycyjnych odpowiedników, co może prowadzić do powstania warunków zagrażających bezpieczeństwu [Gar05]. Na przykład, stronicowanie, sprawdzanie punktowe i migracja maszyn wirtualnych mogą powodować wyciek wrażliwych danych do pamięci trwałej, przełamując mechanizmy ochrony w hostowanym systemie operacyjnym, mające na celu zapobieganie takim zdarzeniom. Ponadto, sam hiperwizor może zostać potencjalnie skompromitowany. Kompromitacja hiperwizora może skutkować naruszeniem wszystkich systemów, które są przez niego hostowane [Sca11]. Na przykład, luka pozwalająca specjalnie spreparowanym żądaniom FTP (File Transfer Protocol) na uszkodzenie bufora stosu w hiperwizorze, który z kolei może spowodować wykonanie dowolnego kodu na hoście, została odkryta w procedurze NAT (Network Address Translation) powszechnie używanego oprogramowania do wirtualizacji [Sec05, She05].
Wirtualne serwery i aplikacje, podobnie jak ich niewirtualne odpowiedniki, muszą być zabezpieczone zarówno fizycznie jak i logicznie. Zgodnie z politykami i procedurami organizacyjnymi, system operacyjny i aplikacje powinny być specjalnie zabezpieczone (utwardzone) podczas tworzenia implementacji obrazów maszyn wirtualnych. Należy również zadbać o zapewnienie bezpieczeństwa środowiskom zwirtualizowanym, w których obrazy są uruchamiane [You07]. Na przykład, wirtualne zapory sieciowe mogą być użyte do odizolowania grup maszyn wirtualnych od innych grup hostowanych, takich jak systemy produkcyjne od systemów deweloperskich lub systemy deweloperskie od innych systemów rezydujących w chmurze. Precyzyjne zarządzanie obrazami maszyn wirtualnych jest również istotne, aby uniknąć

przypadkowego wdrożenia obrazów w fazie rozwoju lub też zawierających luki w zabezpieczeniach.

Ochrona sieci wirtualnej. Większość platform wirtualizacyjnych ma możliwość tworzenia programowych przełączników i konfiguracji sieciowych jako części środowiska wirtualnego, aby umożliwić maszynom wirtualnym na tym samym hoście bardziej bezpośrednią i wydajną komunikację. Na przykład, w przypadku maszyn wirtualnych, które nie wymagają dostępu do sieci zewnętrznej, architektury sieci wirtualnych większości oprogramowania do wirtualizacji obsługują sieci typu "intra-host", w których tworzona jest prywatna podsieć do komunikacji wewnątrz hosta. Ruch w sieciach wirtualnych może nie być widoczny dla urządzeń zabezpieczających w sieci fizycznej, takich jak sieciowe systemy wykrywania i zapobiegania włamaniom [Sca11, Vie09]. W celu uniknięcia utraty widoczności i ochrony przed atakami wewnątrz hosta, może być wymagane powielenie możliwości ochrony sieci fizycznej w sieci wirtualnej [Ref10, Vmw10]. Chociaż niektóre hiperwizory umożliwiają monitorowanie sieci, ich możliwości nie są na ogół tak rozbudowane, jak w przypadku narzędzi używanych do monitorowania sieci fizycznych. Organizacje powinny rozważyć ryzyko i wydajność pomiędzy ukryciem ruchu w hiperwizorze, a ujawnieniem tego ruchu w sieci fizycznej w celu monitorowania [Sca11].

Efektem ubocznym środowisk zwirtualizowanych jest potencjalna utrata możliwości rozdzielenia obowiązków pomiędzy istniejącymi w organizacji rolami administracyjnymi. Na przykład, w tradycyjnych środowiskach komputerowych administratorzy komputerów zazwyczaj nie konfigurują komponentów bezpieczeństwa sieciowego, takich jak systemy wykrywania i zapobiegania włamaniom oraz zapory sieciowe. Z drugiej strony, administratorzy bezpieczeństwa sieci mogą konfigurować takie urządzenia, ale zazwyczaj nie mają praw administracyjnych na hostach, aby przyznać dostęp do systemu. W środowiskach wirtualnych odrębne role administratorów bezpieczeństwa komputerowego i sieciowego mogą zostać połączone w jedną rolę administratora infrastruktury wirtualnej. Podobnie może to mieć wpływ na inne odrębne role, takie jak role administratorów pamięci masowej. Zabezpieczenia zarządzania i operacyjne mogą być konieczne, aby zrekompensować brak zabezpieczeń technicznych w środowiskach wirtualnych zapewniających rozdzielenie obowiązków.

Obrazy maszyn wirtualnych. Dostawcy chmur IaaS oraz wytwórcy maszyn wirtualnych utrzymują repozytoria obrazów maszyn wirtualnych. Obraz maszyny wirtualnej obejmuje stos oprogramowania, w tym zainstalowane i skonfigurowane aplikacje, używane do załadowania maszyny wirtualnej do stanu początkowego lub stanu z poprzedniego punktu sprawdzającego. Udostępnianie obrazów maszyn wirtualnych jest powszechną praktyką w niektórych środowiskach chmury obliczeniowej i stanowi szybki sposób na uruchomienie. Obrazy maszyn wirtualnych tworzone przez organizację muszą być starannie zarządzane i kontrolowane, w celu uniknięcia problemów. Na przykład, obrazy muszą być na bieżąco aktualizowane najnowszymi poprawkami bezpieczeństwa. Należy uważać, aby nie używać obrazów, które nie zostały zweryfikowane lub nie są udostępniane w sposób przypadkowy. Dostawca obrazu jest narażony na ryzyko, ponieważ obraz może zawierać zastrzeżony kod i dane oraz zawierać luki w zabezpieczeniach. Atakujący może próbować badać obrazy, aby ustalić, czy nie wyciekają z nich informacje lub czy nie stanowią one drogi do ataku [Wei09]. Jest to szczególnie istotne w przypadku obrazów deweloperskich, które są udostępniane incydentalnie. Atakujący może również próbować dostarczyć obraz maszyny wirtualnej zawierający złośliwe oprogramowanie odbiorcom usługi przetwarzania w chmurze [Jen09, Wei09].[16] Na przykład, badający zademonstrowali, że manipulując procesem rejestracji w celu uzyskania pierwszej pozycji na liście, mogli łatwo nakłonić odbiorców usługi w chmurze do uruchomienia obrazów maszyn wirtualnych, które sami udostępnili w repozytorium obrazów popularnego dostawcy usług w chmurze [Mee09, Sla09]. Ryzyko dla odbiorców korzystających ze skażonych obrazów obejmuje kradzież i uszkodzenie danych. Organizacje powinny rozważyć wdrożenie sformalizowanego procesu zarządzania obrazami, aby regulować tworzenie, przechowywanie i korzystanie z obrazów maszyn wirtualnych [Sca11].

Ochrona po stronie klienta. Skuteczna obrona przed atakami wymaga zabezpieczenia zarówno po stronie serwera chmury obliczeniowej, jak i klienta. Przy nacisku

[16] Dla środowisk PaaS i SaaS dostarczany jest złośliwy moduł wdrożeniowy.

kładzionym zazwyczaj na tę pierwszą, drugą można łatwo przeoczyć. Usługi od różnych dostawców chmury, jak również aplikacje oparte na chmurze stworzone przez organizację, mogą nakładać bardziej wymagające wymagania na klienta, co może mieć wpływ na bezpieczeństwo i ochronę prywatności, które muszą być wzięte pod uwagę. Przeglądarki internetowe, kluczowy element dla wielu usług chmury obliczeniowej, oraz różne dostępne dla nich wtyczki i rozszerzenia cieszą się złą sławą ze względu na problemy z bezpieczeństwem [Jen09, Ker10, Pro07, Pro09]. Co więcej, wiele dodatków do przeglądarek nie zapewnia automatycznych aktualizacji, co zwiększa trwałość wszelkich istniejących luk.

Utrzymanie fizycznego i logicznego bezpieczeństwa nad klientami może być kłopotliwe, szczególnie w przypadku wbudowanych urządzeń mobilnych, takich jak smartfony. Ich rozmiar i przenośność mogą spowodować utratę fizycznej kontroli. Wbudowane mechanizmy bezpieczeństwa często nie są wykorzystywane lub mogą być bez trudu pokonane lub ominięte przez dobrze zorientowaną osobę w celu przejęcia kontroli nad urządzeniem [Jan08]. Smartfony są również traktowane bardziej jako urządzenia stacjonarne z ograniczonym zestawem funkcji, niż jako systemy ogólnego przeznaczenia. Ponadto, aplikacje w chmurze są często dostarczane do nich za pośrednictwem tworzonych na zamówienie aplikacji natywnych, a nie przeglądarki internetowej. Żaden pojedynczy system operacyjny nie dominuje w smartfonach, a poprawki i aktualizacje bezpieczeństwa dla komponentów systemu nie są tak częste jak w przypadku komputerów stacjonarnych, co sprawia, że luki są bardziej trwałe i poszerzają okno możliwości ich wykorzystania. Jako zabezpieczenie, organizacje mogą zabronić lub ściśle ograniczyć dostęp do informacji osobistych i innych wrażliwych danych z urządzeń przenośnych i mobilnych zmniejszając tym samym ryzyko [Mcc10].

Rosnąca dostępność i wykorzystanie mediów społecznościowych, poczty elektronicznej i innych publicznie dostępnych stron również wiąże się z zagrożeniami, które są powodem do niepokoju, ponieważ coraz częściej służą one jako miejsca ataków socjotechnicznych, które mogą mieć negatywny wpływ na bezpieczeństwo przeglądarki, jej platformy bazowej i usług w chmurze, do których uzyskuje się dostęp. Na przykład, oprogramowanie szpiegujące zostało podobno zainstalowane w systemie

szpitalnym poprzez osobiste konto Webmail pracownika i wysłało atakującemu ponad 1000 zrzutów ekranu, zawierających informacje finansowe i inne poufne informacje, zanim zostało wykryte [Mcm09b]. Posiadanie trojana backdoor, rejestratora naciśnięć klawiszy lub innego rodzaju złośliwego oprogramowania obecnego na kliencie jest sprzeczne z ochroną bezpieczeństwa i prywatności usług chmury publicznej, jak również innych usług publicznych dostępnych przez Internet [Fre08, MRG10].
Jako część ogólnej architektury bezpieczeństwa przetwarzania w chmurze, organizacje muszą dokonać przeglądu istniejących środków i zastosować dodatkowe, jeśli jest to konieczne, aby zabezpieczyć stronę klienta. Banki zaczynają odgrywać wiodącą rolę we wdrażaniu wzmocnionych środowisk przeglądarek, które szyfrują wymianę danych w sieci i chronią przed rejestrowaniem naciśnięć klawiszy [Dun10a, Dun10b]. Szkolenie w zakresie świadomości bezpieczeństwa jest również ważnym środkiem do zastosowania przez organizację, ponieważ właściwe zachowanie ludzi jest istotnym zabezpieczeniem przed wieloma rodzajami ataków.

4.5. ZARZĄDZANIE TOŻSAMOŚCIĄ I DOSTĘPEM

Wrażliwość danych i prywatność informacji stają się coraz częściej przedmiotem szczególnej uwagi organizacji. Aspekty potwierdzania tożsamości i uwierzytelniania w ramach zarządzania tożsamością wiążą się z wykorzystaniem, utrzymaniem i ochroną danych osobowych uzyskanych od użytkowników. Zapobieganie nieautoryzowanemu dostępowi do zasobów informacyjnych w chmurze jest również istotnym zagadnieniem. Jednym z powtarzających się problemów jest to, że organizacyjne ramy identyfikacji i uwierzytelniania mogą w żaden sposób nie obejmować chmury publicznej, a rozszerzenie lub zmiana istniejących ram w celu wsparcia usług w chmurze może okazać się utrudnione [Cho09]. Alternatywa polegająca na stosowaniu dwóch różnych systemów uwierzytelniania, jednego dla wewnętrznych systemów organizacyjnych i drugiego dla zewnętrznych systemów opartych na chmurze, jest utrudnieniem, które z czasem może stać się niewykonalne. Jednym z rozwiązań jest federacja tożsamości, spopularyzowana wraz z wprowadzeniem architektury zorientowanej na usługi.

Federacja tożsamości pozwala organizacji i dostawcy chmury na zaufanie i współdzielenie cyfrowych tożsamości i atrybutów w obu domenach, a także na zapewnienie sposobu pojedynczego logowania. Aby federacja odniosła sukces, transakcje zarządzania tożsamością i dostępem muszą być interpretowane precyzyjnie i jednoznacznie oraz chronione przed atakami. Należy również zapewnić wyraźne oddzielenie zarządzanych tożsamości odbiorcy chmury od tożsamości dostawcy chmury, aby chronić zasoby odbiorcy przed podmiotami uwierzytelnionymi przez dostawcę i odwrotnie. Federacja tożsamości może być zrealizowana na wiele sposobów, np. za pomocą standardu Security Assertion Markup Language (SAML)[17] lub standardu OpenID.

- **Uwierzytelnianie.** Uwierzytelnianie jest procesem ustanawiania wiarygodności tożsamości użytkowników. Poziomy pewności uwierzytelniania powinny być odpowiednie do wrażliwości aplikacji i zasobów informacyjnych, do których uzyskuje się dostęp oraz związanego z tym ryzyka [Bur06]. Coraz większa liczba dostawców usług w chmurze wspiera standard SAML i wykorzystuje go do administrowania użytkownikami i uwierzytelniania ich przed zapewnieniem dostępu do aplikacji i danych. SAML dostarcza środków do wymiany informacji pomiędzy współpracującymi domenami. Na przykład, transakcja SAML może przekazywać potwierdzenie, że użytkownik został uwierzytelniony przez dostawcę tożsamości, a także zawierać informacje o uprawnieniach użytkownika. Po przyjęciu transakcji, dostawca usług wykorzystuje te informacje do przyznania użytkownikowi odpowiedniego poziomu dostępu, po pomyślnym zweryfikowaniu tożsamości i poświadczeń dostarczonych dla użytkownika.
  Komunikaty żądania i odpowiedzi SAML są zazwyczaj odwzorowywane za pomocą protokołu SOAP, którego format opiera się na języku XML (eXtensible Markup Language). Wiadomości SOAP są podpisywane cyfrowo. Na przykład w chmurze

[17] Patrz: publikacja NSC 7298.

publicznej, gdy użytkownik ustanowił z daną usługą certyfikat klucza publicznego, klucz prywatny może być użyty do podpisania żądań SOAP.
Walidacja bezpieczeństwa wiadomości SOAP jest skomplikowana i musi być przeprowadzona precyzyjnie, aby zapobiec atakom. Ataki typu "zawijanie XML" (*ang. XML wrapping*) zostały z powodzeniem przeprowadzone przeciwko publicznej chmurze IaaS [Gru09]. Zawijanie XML polega na manipulacji wiadomościami SOAP. Nowy element (tj. wrapper) jest wprowadzany do nagłówka SOAP Security; oryginalne treści wiadomości są następnie przenoszone pod wrapper i zastępowane przez fałszywe treści zawierające operację zdefiniowaną przez atakującego [Gaj09, Gru09]. Do oryginalnego obiektu nadal można się odwoływać i weryfikować jego sygnaturę, ale zamiast niego wykonywana jest operacja zawarta w obiekcie zastępczym.

- **Kontrola dostępu.** Do świadczenia usług zarządzania tożsamością i dostępem w chmurze tylko sam SAML nie jest wystarczający. Potrzebna jest również zdolność do dostosowania uprawnień odbiorców chmury i zapewnienia kontroli nad dostępem do zasobów. W ramach zarządzania tożsamością, standardy takie jak eXtensible Access Control Markup Language (XACML)[18] mogą być wykorzystywane przez dostawcę chmury do kontroli dostępu do zasobów chmury, zamiast niektórych zastrzeżonych rozwiązań. Standard XACML definiuje oparty na XML język do określania polityki i formowania decyzji kontroli dostępu. XACML skupia się na mechanizmie dochodzenia do decyzji autoryzacyjnych, co uzupełnia SAML skupiający się na środkach przekazywania decyzji uwierzytelniających i autoryzacyjnych pomiędzy współpracującymi podmiotami.
  XACML jest w stanie kontrolować zastrzeżone interfejsy usług większości dostawców, dlatego niektórzy dostawcy chmur już go stosują. Podstawowy model użycia XACML zakłada, że gdy podejmowana jest próba dostępu do zasobu, Punkt Realizacji Zasad (ang. Policy Enforcement Point - PEP), odpowiedzialny za ochronę

[18] Patrz: publikacja NSC 7298.

dostępu do zasobów, wysyła żądanie zawierające opis próby dostępu do Punktu Decyzyjnego Zasad (ang. Policy Decision Point - PDP) w celu oceny pod kątem dostępnych polityk i atrybutów. PDP ocenia to żądanie i zwraca decyzję o autoryzacji, którą PEP może egzekwować. XACML nie definiuje protokołów lub mechanizmów transportowych ani nie określa sposobu walidacji danych uwierzytelniających użytkownika. Komunikaty przesyłane pomiędzy podmiotami XACML są podatne na ataki złośliwych stron trzecich, w tym ataki nieautoryzowanego ujawnienia, powtórzenia, usunięcia i modyfikacji, chyba, że istnieją wystarczające zabezpieczenia do ochrony transakcji [Kel05].

4.6. IZOLACJA OPROGRAMOWANIA

Wysoki stopień współużytkowania wielu platform jest konieczny dla przetwarzania w chmurze, aby osiągnąć przewidywaną elastyczność dostarczania niezawodnych usług na żądanie oraz korzyści kosztowe i wydajnościowe wynikające z ekonomii skali. Aby osiągnąć pożądane wysokie wskaźniki konsumpcji, dostawcy chmury muszą zapewnić dynamiczne, elastyczne dostarczanie usług i odizolowanie zasobów odbiorców usług chmurowych. Współużytkowanie w środowiskach chmury obliczeniowej IaaS odbywa się zazwyczaj poprzez multipleksowanie działania maszyn wirtualnych od potencjalnie różnych odbiorców na tym samym serwerze fizycznym [Ris09]. Aplikacje wdrożone na wirtualnych maszynach gościnnych pozostają podatne na ataki i kompromitację, podobnie jak ich niezwirtualizowane odpowiedniki. Dramatycznym tego przykładem był botnet działający w środowisku chmury obliczeniowej IaaS [Mcm09a, Whi09].

Wielodostęp w środowiskach PaaS i SaaS chmury obliczeniowej może być traktowana w różny sposób. Na przykład, wielu dostawców SaaS opiera się na infrastrukturze niezawierającej maszyn wirtualnych, używając zamiast tego pojedynczej logicznej instancji aplikacji (tj. stosu technologii oprogramowania), która może obsługiwać bardzo dużą liczbę najemców, przeskalowując ją w górę lub na zewnątrz w zależności od potrzeb [Arm10, Wai08]. Niezależnie od zastosowanego modelu usług i architektury oprogramowania przeznaczonego dla wielodostępu, przetwarzanie danych przez

różnych odbiorców musi być możliwe do przeprowadzenia w izolacji od siebie, głównie poprzez zastosowanie mechanizmów separacji logicznej.

- **Złożoność hiperwizora.** Bezpieczeństwo systemu komputerowego zależy od jakości kernela oprogramowania, które kontroluje ograniczanie i wykonywanie procesów. Monitor maszyn wirtualnych lub hiperwizor jest zaprojektowany do jednoczesnego uruchamiania wielu maszyn wirtualnych, z których każda na jednym komputerze-hoście zawiera system operacyjny i aplikacje, oraz do zapewnienia izolacji pomiędzy różnymi maszynami wirtualnymi gości.
  Monitor maszyny wirtualnej może być teoretycznie „mniejszy" i mniej złożony niż system operacyjny. Te cechy generalnie ułatwiają analizę i poprawiają jakość zabezpieczeń, dając monitorowi maszyny wirtualnej potencjał do bycia lepiej dostosowanym do utrzymywania silnej izolacji pomiędzy maszynami wirtualnymi gości niż system operacyjny do izolowania procesów [Kar08]. W praktyce jednak, nowoczesne hiperwizory mogą być duże i złożone, porównywalne do systemu operacyjnego, co neguje tę zaletę. Na przykład Xen, open source'owy monitor maszyn wirtualnych x86, zawiera zmodyfikowane jądro Linuksa w celu implementacji uprzywilejowanej partycji dla operacji wejścia/wyjścia, a KVM, kolejny projekt open source, przekształca jądro Linuksa w monitor maszyn wirtualnych [Kar08, Sha08, Xen08]. Zrozumienie wykorzystania wirtualizacji przez dostawcę chmury jest warunkiem wstępnym do poznania związanego z nią ryzyka bezpieczeństwa.
- **Wektory ataku.** Wielodostępność w infrastrukturach chmur opartych na maszynach wirtualnych, wraz z subtelnościami w sposobie, w jaki zasoby fizyczne są współdzielone pomiędzy maszynami wirtualnymi gościa, może rodzić nowe źródła zagrożeń. Najpoważniejszym zagrożeniem jest to, że złośliwy kod może wydostać się z granic swojej wirtualnej maszyny i zakłócić działanie hiperwizora lub innych maszyn wirtualnych gościa. Migracja na żywo, możliwość przenoszenia maszyny wirtualnej pomiędzy hiperwizorami na różnych komputerach bez zatrzymywania systemu operacyjnego gościa, oraz inne funkcje udostępniane przez środowiska monitorujące maszyny wirtualne w celu ułatwienia zarządzania

systemami, również zwiększają rozmiar i złożoność oprogramowania oraz potencjalnie dodają kolejne obszary, które mogą stać się celem ataku.
Kilka przykładów ilustruje rodzaje możliwych wektorów ataku. Pierwszym z nich jest mapowanie infrastruktury chmury. Choć wydaje się to trudne do wykonania zadanie, badacze zademonstrowali podejście do popularnej chmury IaaS [Ris09]. Uruchamiając wiele instancji maszyn wirtualnych z wielu kont odbiorców chmury i wykorzystując sondy sieciowe, przeanalizowano przypisane adresy IP i nazwy domen w celu zidentyfikowania wzorców lokalizacji usług. W oparciu o te informacje i ogólną metodologię, można było zidentyfikować prawdopodobną lokalizację konkretnej docelowej maszyny wirtualnej i utworzyć nowe maszyny wirtualne, które docelowo będą współrezydentami maszyny docelowej.
Po znalezieniu odpowiedniego miejsca docelowego, następnym krokiem dla maszyny wirtualnej gościa jest ominięcie lub przełamanie zabezpieczeń hiperwizora lub całkowite zniszczenie hiperwizora i systemu. Podatności w dostarczonych interfejsach programowania i przetwarzaniu poleceń są powszechnymi celami do wykrycia podatności do wykorzystania [Fer07]. Na przykład, poważna luka, która pozwalała atakującemu na zapis do dowolnego miejsca w pamięci nieobjętej granicami, została odkryta w kodzie zarządzania energią hiperwizora poprzez testowanie odporności na błędne dane z emulowanych portów I/O [Orm07].15 Luka w mechanizmie odmowy usługi (DoS), która może pozwolić wirtualnej maszynie gościa na uszkodzenie komputera-hosta wraz z innymi hostowanymi maszynami wirtualnymi, została również odkryta w sterowniku urządzeń wirtualnych popularnego oprogramowania do wirtualizacji [Vmw09].
Możliwe są również bardziej pośrednie drogi ataku. Na przykład, badacze opracowali sposób, w jaki atakujący może uzyskać kontrolę administracyjną nad maszynami wirtualnymi gościa podczas migracji na żywo, poprzez wykorzystanie ataku man-in-the-middle do modyfikacji kodu używanego do uwierzytelniania [Obe08a]. Modyfikacja pamięci podczas migracji stwarza inne możliwości, takie jak możliwość umieszczenia warstwy rootkitów opartych na maszynie wirtualnej pod systemem operacyjnym [Kin06]. Exploit zero-day w HyperVM, aplikacji open

source do zarządzania wirtualnymi serwerami prywatnymi, rzekomo doprowadził do zniszczenia około 100 000 stron internetowych opartych na serwerach wirtualnych hostowanych przez dostawcę usług [Goo09b]. Inny przykład ataku pośredniego polega na monitorowaniu wykorzystania zasobów na serwerze współdzielonym w celu zdobycia informacji i być może przeprowadzenia ataku typu side-channel, podobnego do ataków stosowanych przeciwko implementacjom mechanizmów kryptograficznych w innych środowiskach obliczeniowych [Ris09]. Na przykład, atakujący mógłby określić okresy wysokiej aktywności, oszacować wysoki poziom ruchu i ewentualnie przeprowadzić ataki na czas naciskania klawiszy w celu zebrania haseł i innych danych z serwera docelowego.

4.7. OCHRONA DANYCH

Dane przechowywane w chmurze publicznej zazwyczaj rezydują we współdzielonym środowisku kolokowanym z danymi innych klientów. Organizacje umieszczające wrażliwe i regulowane dane w chmurze publicznej muszą zatem uwzględnić środki, za pomocą których dostęp do danych jest kontrolowany, a dane są przetwarzane w bezpiecznym środowisku. Podobne obawy istnieją w przypadku danych migrowanych w ramach chmury lub pomiędzy chmurami.

- **Koncentracja wartości.** Odpowiedź na pytanie "Dlaczego napadasz na banki?" jest często przypisywana Williemu Suttonowi, historycznemu i wielokrotnemu rabusiowi banków [Coc97] - jego rzekoma odpowiedź brzmi: "ponieważ tam są pieniądze". Na wiele sposobów, zapisy danych są walutą XXI wieku, a oparte na chmurze magazyny danych są bankowym skarbcem, czyniąc je coraz bardziej pożądanym celem ze względu na zbiorową wartość tam skoncentrowaną [Row07]. Podobnie jak ekonomia skali istnieje w przypadku okradania banków zamiast pojedynczych osób, wysoki współczynnik opłacalności istnieje również w przypadku skutecznego kompromitowania chmury. Udane exploity przeciwko wysoko cenionym firmom zajmującym się bezpieczeństwem ilustrują, że nikt nie jest poza zasięgiem zdeterminowanego przeciwnika (np. [And11], [Bra11] i [Pep11b]).

W przeciwieństwie do bezpośredniego podejścia, znakiem rozpoznawczym Williego było połączenie finezji i przebiegłości Ten styl działa równie dobrze w cyfrowym świecie przetwarzania w chmurze. Na przykład, niedawny exploit obejmował namierzenie osobistego konta poczty elektronicznej administratora serwisu społecznościowego, podobno poprzez udzielenie odpowiedzi na zestaw pytań bezpieczeństwa w celu uzyskania dostępu do konta, a następnie wykorzystanie znalezionych tam informacji w celu uzyskania dostępu do plików firmowych przechowywanych w chmurze PaaS [Inf09, Sut09]. Podobny słaby punkt w resetowaniu haseł został zidentyfikowany w chmurze publicznej IaaS [Gar07]. Zarejestrowany adres poczty elektronicznej i ważne hasło do konta były wszystkim, co było wymagane do pobrania poświadczeń uwierzytelniających z pulpitu zarządzania dostawcy chmury, co z kolei dawało dostęp do wszystkich zasobów konta. Ponieważ utracone hasła do usługi w chmurze mogły być resetowane za pomocą poczty elektronicznej, atakujący kontrolujący system pocztowy powiązany z kontem lub pasywnie podsłuchujący sieć, przez którą przechodziła poczta elektroniczna zawierająca reset hasła, mógł skutecznie przejąć kontrolę nad kontem.

Posiadanie danych kolokowanych z danymi organizacji o wysokim profilu zagrożenia może również prowadzić do odmowy usługi, jako niezamierzona przyczyna ataku skierowanego przeciwko tej organizacji [Row07]. Podobnie, skutki uboczne fizycznego ataku na zasoby chmurowe organizacji o wysokim profilu są również możliwe. Na przykład, przez lata obiekty urzędów podatkowych przyciągały uwagę potencjalnych napastników [Kat10, Lab95, Lat96, Sch10].

- **Izolowanie danych.** Dane mogą występować w wielu formach. Na przykład, w przypadku tworzenia aplikacji w chmurze, obejmują one programy aplikacji, skrypty i ustawienia konfiguracyjne wraz z narzędziami deweloperskimi. W przypadku wdrożonych aplikacji obejmują one rekordy i inną zawartość utworzoną lub używaną przez aplikacje, w tym obiekty przenoszone, a także informacje o kontach użytkowników aplikacji. Kontrola dostępu jest jednym ze sposobów ochrony danych przed nieuprawnionymi użytkownikami; kolejnym środkiem jest szyfrowanie. Kontrole dostępu są zazwyczaj oparte na identyfikacji,

co sprawia, że uwierzytelnianie tożsamości użytkownika jest istotnym zagadnieniem w chmurach obliczeniowych. W przypadku braku fizycznej kontroli nad przechowywaniem informacji, szyfrowanie jest jedynym sposobem zapewnienia, że są one rzeczywiście chronione.

Środowiska bazodanowe wykorzystywane w chmurze obliczeniowej mogą się znacząco różnić. Na przykład, niektóre środowiska wspierają model wieloinstancyjny (*ang. multi-instance*), podczas gdy inne wspierają model wielodostępowy (*ang. multi-tenant*). Te pierwsze zapewniają unikalny system zarządzania bazą danych działający na instancji maszyny wirtualnej dla każdego odbiorcy chmury, dając odbiorcy pełną kontrolę nad definiowaniem ról, autoryzacją użytkowników i innymi zadaniami administracyjnymi związanymi z bezpieczeństwem. Te drugie zapewniają predefiniowane środowisko dla odbiorcy chmury, które jest współdzielone z innymi dzierżawcami, zazwyczaj poprzez tagowanie danych identyfikatorem odbiorcy. Tagowanie daje poczucie wyłącznego korzystania z instancji, ale opiera się na dostawcy chmury w celu ustanowienia i utrzymania solidnego bezpiecznego środowiska bazy danych.

Istnieją różne rodzaje aranżacji wielodostępu dla baz danych. Każdy układ łączy zasoby w inny sposób, oferując różne stopnie izolacji i wydajności zasobów [Jac07, Wai08]. Istnieją również inne uwarunkowania. Na przykład, niektóre funkcje, takie jak szyfrowanie danych, są bardziej efektywne w układach, które wykorzystują oddzielne, a nie wspólne bazy danych. Tego rodzaju zestawienia wymagają starannej oceny przydatności rozwiązania do zarządzania danymi w odniesieniu do danych, których dotyczą. Wymagania w niektórych dziedzinach lub branżach, takich jak służba zdrowia, mogą mieć wpływ na wybór bazy danych i organizacji danych wykorzystywanych w aplikacji. Poważnym problemem jest ogólnie pojęta ochrona prywatności informacji [Pea09].

Dane muszą być zabezpieczone w stanie spoczynku, w tranzycie i podczas użytkowania, a dostęp do nich musi być kontrolowany. Standardy protokołów komunikacyjnych i certyfikatów klucza publicznego pozwalają na ochronę transferów danych za pomocą kryptografii i mogą być zazwyczaj wdrażane z równym powodzeniem w środowiskach SaaS, PaaS i IaaS [CSA11a, Pro10].

Procedury ochrony danych w spoczynku nie są jednak tak dobrze ustandaryzowane, co sprawia, że interoperacyjność jest problemem ze względu na przewagę systemów prawnie zastrzeżonych. Zdolność ochrony różni się również znacznie w zależności od modelu usług, a ochrona kryptograficzna może być niewykonalna dla niektórych środowisk, w szczególności PaaS i SaaS [CSA11a, Pro10]. Brak interoperacyjności wpływa na dostępność danych i komplikuje możliwość przenoszenia aplikacji i danych pomiędzy dostawcami chmury. Ochrona danych w użyciu jest rozwijającym się obszarem kryptografii z niewielką ilością praktycznych rezultatów do zaoferowania, pozostawiając mechanizmy zaufania jako główne zabezpieczenie [Gre09, Pro10].

Bezpieczeństwo systemu wykorzystującego kryptografię zależy od właściwego zabezpieczenia kluczy centralnych i komponentów zarządzania kluczami [Bar05]. Obecnie odpowiedzialność za zarządzanie kluczami kryptograficznymi spoczywa głównie na odbiorcy chmury. Generowanie i przechowywanie kluczy odbywa się zazwyczaj poza chmurą z wykorzystaniem sprzętowych modułów bezpieczeństwa, które nie skalują się dobrze do paradygmatu chmury. Projekt Zarządzania Kluczami Kryptograficznymi NIST (NIST's Cryptographic Key Management Project[19]) identyfikuje skalowalne i użyteczne strategie zarządzania i wymiany kluczy kryptograficznych do wykorzystania przez rząd, co może pomóc w ostatecznym złagodzeniu problemu[20].

Zasadą nadrzędną jest, aby to właśnie personel organizacji sprawował kontrolę nad centralnym materiałem kluczy i konfigurował komponenty zarządzania kluczami w aplikacjach opartych na chmurze [Bar05]. Przed podjęciem działań w środowiskach chmurowych, w których dostawca chmury zapewnia udogodnienia do zarządzania kluczami, organizacja musi w pełni zrozumieć i rozważyć ryzyko związane z procesami zdefiniowanymi przez dostawcę chmury dotyczącymi cyklu życia zarządzania kluczami [SCA11]. Operacje kryptograficzne wykonywane

[19] http://csrc.nist.gov/groups/ST/keymgmt/

[20] Przywołane przepisy i regulacje odnoszą się do środowiska amerykańskiego i nie mają zastosowania na rynku polskim. Zostały podane jako przykład dla zainteresowanych, chcących poszerzyć swoją wiedzę.

w chmurze stają się częścią procesu zarządzania kluczami i dlatego powinny być zarządzane i audytowane przez organizację.

- **Sanityzacja danych.** Praktyki sanityzacji danych, które dostawca usługi w chmurze wdraża, mają oczywiste implikacje dla bezpieczeństwa. Sanityzacja obejmuje usunięcie danych z nośników pamięci masowej przez nadpisanie, rozmagnesowanie lub inne środki, lub zniszczenie samego nośnika, w celu zapobieżenia nieautoryzowanemu ujawnieniu informacji.[21] Stosuje się ją w różnych sytuacjach odświeżania lub konserwacji sprzętu, np. gdy urządzenie pamięci masowej jest wycofywane z użytku lub ponownie wykorzystywane. Sanityzacja danych dotyczy również kopii zapasowych wykonywanych w celu odzyskania i przywrócenia usługi oraz danych szczątkowych pozostałych po zakończeniu usługi.
  W środowisku publicznej chmury obliczeniowej dane jednego odbiorcy usług chmurowych są fizycznie kolokowane (np. w magazynie danych IaaS) lub zmieszane (np. w bazie danych SaaS) z danymi innych odbiorców, co może komplikować sprawę. Istnieje wiele przykładów pozyskiwania przez analityków używanych dysków z aukcji internetowych i innych źródeł oraz odzyskiwania z nich dużych ilości wrażliwych informacji (np. [Val08]). Przy odpowiednich umiejętnościach i zastosowaniu odpowiedniego sprzętu, możliwe jest również odzyskanie danych z uszkodzonych dysków, jeśli nie są one prawidłowo utylizowane [Sob06]. Umowy o świadczenie usług powinny określać wystarczające środki, które są podejmowane w sposób zapewniający, że sanityzacja danych jest przeprowadzana prawidłowo w całym cyklu życia systemu.

4.8. DOSTĘPNOŚĆ

W uproszczeniu, dostępność to stopień, w jakim pełny zestaw zasobów obliczeniowych organizacji jest dostępny i możliwy do wykorzystania. Dostępność może być zakłócona tymczasowo lub trwale, a utrata może być częściowa lub całkowita. Ataki typu DoS, awarie sprzętu i klęski żywiołowe stanowią zagrożenie dostępności. Problem polega na

[21] Bardziej szczegółowe informacje na temat sanityzacji można znaleźć w dokumencie Guidelines for Media Sanitization (Wytyczne dotyczące sanityzacji nośników) - http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf.

tym, że większość przestojów jest nieplanowana i może mieć wpływ na misję organizacji.

- **Przestoje czasowe.** Pomimo zastosowania architektur zaprojektowanych z myślą o wysokiej niezawodności i dostępności usług, usługi chmury obliczeniowej mogą i doświadczają przestojów i spowolnień wydajności [Lea09]. Istnieje wiele przykładów ilustrujących ten aspekt. W lutym 2008 roku, popularna usługa chmury pamięci masowej doznała trzygodzinnej przerwy w działaniu, która dotknęła jej odbiorców, w tym Twittera i inne firmy startupowe [Dig08, Kri08, Mil08]. W czerwcu 2009 r. burza z piorunami spowodowała częściowy przestój chmury IaaS, który dotknął niektórych użytkowników na cztery godziny, a w kwietniu 2011 r. próba aktualizacji sieci spowodowała poważny przestój trwający ponad dwadzieścia cztery godziny [Met11, Mil09, Pep11a]. Podobnie w lutym 2008 roku awaria klastra bazodanowego w chmurze SaaS spowodowała kilkugodzinną przerwę w działaniu, a w styczniu 2009 roku kolejna krótka przerwa nastąpiła z powodu awarii urządzenia sieciowego [Fer09, Goo09a, Mod08]. W marcu 2009 roku chmura PaaS doświadczyła poważnej degradacji na około dwadzieścia dwie godziny z powodu problemów sieciowych związanych z aktualizacją [Cla09, Mic09]. Przy poziomie dostępności 99,95% należy spodziewać się 4,38 godziny przestoju w ciągu roku. Okresy zaplanowanej konserwacji są zwykle nieuwzględniane jako źródło przestojów w umowach SLA i mogą być zaplanowane z krótkim wyprzedzeniem ze strony dostawcy chmury. Poziom dostępności usługi w chmurze oraz jej możliwości w zakresie tworzenia kopii zapasowych danych i odzyskiwania danych po awarii muszą być uwzględnione w planowaniu awaryjnym i ciągłości działania organizacji, aby zapewnić odzyskiwanie i przywracanie przerwanych usług i operacji w chmurze z wykorzystaniem alternatywnych usług, sprzętu i lokalizacji, jeśli jest to wymagane. Usługi przechowywania danych w chmurze mogą stanowić pojedynczy punkt awarii dla hostowanych tam aplikacji. W takich sytuacjach usługi drugiego dostawcy usług w chmurze mogą być wykorzystywane do tworzenia kopii zapasowych danych przetwarzanych przez głównego dostawcę, aby zapewnić, że podczas długotrwałego zakłócenia lub poważnej awarii

w obiektach głównego dostawcy, dane pozostaną dostępne do natychmiastowego wznowienia krytycznych operacji.

- **Wydłużone i stałe przerwy w działaniu.** Istnieje możliwość, że dostawca chmury może doświadczyć poważnych problemów, takich jak bankructwo lub zamknięcie jednostki, które wpływają na usługi przez dłuższy czas lub powodują całkowite wyłączenie. Na przykład w kwietniu 2009 roku Federalne Biuro Śledcze dokonało nalotu na centra obliczeniowe w Teksasie i przejęło setki serwerów, badając zarzuty oszustwa przeciwko kilku firmom, które działały za pośrednictwem tych centrów [Zet09a]. Zajęcie zakłóciło usługi setek innych firm niezwiązanych ze śledztwem, ale które miały nieszczęście prowadzenia operacji komputerowych w centrach, które były celem tego dochodzenia [Zet09a]. Podobny nalot z podobnym skutkiem miał również miejsce niedawno [Sch11]. Inne przykłady przestojów to poważna utrata danych, jakiej w 2009 r. doświadczyła usługa repozytorium zakładek oraz nagła awaria dostawcy usługi przechowywania danych on-line, który w 2008 r. zamknął działalność bez ostrzeżenia swoich użytkowników [Cal09, Gun08]. Zmieniające się warunki biznesowe mogą również spowodować, że dostawca chmury zrezygnuje ze swoich usług, jak to miało miejsce ostatnio w przypadku usługi przechowywania danych w chmurze online [Sto10]. Jeżeli organizacja polega na usłudze w chmurze w zakresie przechowywania i przetwarzania danych, musi być przygotowana do prowadzenia krytycznych dla misji operacji bez korzystania z usługi w okresach, gdy chmura doświadcza poważnego przestoju. Plan awaryjny organizacji powinien uwzględniać długotrwałe i stałe zakłócenia systemu oraz wspierać ciągłość operacji, które skutkują przywróceniem istotnych funkcji w innym miejscu. Posiadanie polityki, planów i standardowych procedur operacyjnych pozwala na uniknięcie tworzenia nadmiernej zależności od korzystania z usług w chmurze bez wystarczającej rekompensaty.
- **Odmowa usługi (Denial of Service – DoS).** Atak typu denial of service polega na zasypaniu celu fałszywymi żądaniami, aby uniemożliwić mu terminowe odpowiadanie na uzasadnione żądania. Atakujący zazwyczaj wykorzystuje wiele komputerów lub botnet do przeprowadzenia ataku. Nawet nieudany rozproszony

atak odmowy usługi może szybko pochłonąć duże ilości zasobów, aby się przed nim bronić i spowodować gwałtowny wzrost opłat. Dynamiczne udostępnianie chmury w pewien sposób upraszcza pracę atakującego w celu wyrządzenia szkody. Podczas, gdy zasoby chmury są znaczące, z wystarczającą liczbą atakujących komputerów mogą zostać przeciążone [Jen09]. Na przykład, atak typu DoS na stronę hostującą kod działającą w chmurze IaaS spowodował ponad 19 godzin przestoju [Bro09, Met09].

Oprócz ataków na publicznie dostępne usługi dostępne przez Internet, ataki typu DoS mogą być skierowane przeciwko wewnętrznie dostępnym usługom, takim jak te wykorzystywane w zarządzaniu chmurą [Mee09, Sla09]. Wewnętrznie przypisane adresy nieroutowane, wykorzystywane do zarządzania zasobami w sieci dostawcy chmury, również mogą być wykorzystane jako wektor ataku.

W najgorszym przypadku istnieje możliwość, że elementy jednej chmury zaatakują elementy innej chmury lub zaatakują niektóre z własnych elementów [Jen09].

4.9. REAKCJA NA INCYDENTY

Jak sama nazwa wskazuje, reakcja na incydent polega na zorganizowaniu metody postępowania z konsekwencjami ataku na bezpieczeństwo systemu komputerowego. Rola dostawcy chmury jest kluczowa w wykonywaniu działań reagowania na incydenty, w tym weryfikacji incydentu, analizy ataku, powstrzymywania, zbierania i zachowywania danych, remediacji problemu i przywracania usług. Każda warstwa w stosie aplikacji w chmurze, w tym aplikacja, system operacyjny, sieć i baza danych, generuje dzienniki zdarzeń, podobnie jak inne komponenty chmury, takie jak load balancery i systemy wykrywania włamań; wiele takich źródeł zdarzeń i sposoby dostępu do nich są pod kontrolą dostawcy chmury.

Złożoność usługi w chmurze może utrudniać rozpoznanie i analizę incydentów. Na przykład, jeden z dostawców IaaS potrzebował około ośmiu godzin, aby rozpoznać i rozpocząć działania w związku z oczywistym atakiem typu DoS na jego infrastrukturę chmurową, po tym jak problem został zgłoszony przez odbiorcę usługi [Bro09, Met09]. Aktualizacja planu reagowania na incydenty w organizacji w celu uwzględnienia różnic pomiędzy organizacyjnym środowiskiem przetwarzania, a środowiskiem przetwarzania

w chmurze jest istotnym, ale łatwym do przeoczenia warunkiem wstępnym do przeniesienia aplikacji i danych.

- **Dostępność danych.** Dostępność istotnych danych z monitorowania zdarzeń jest niezbędna do wykrywania incydentów bezpieczeństwa w odpowiednim czasie. Odbiorcy chmury często mają do czynienia z bardzo ograniczonymi możliwościami wykrywania incydentów w środowiskach chmury publicznej [Gro10]. Najważniejsze problemy obejmują niewystarczający dostęp do źródeł zdarzeń i informacji o podatnościach pozostających pod kontrolą dostawcy chmury, nieodpowiednie interfejsy umożliwiające dostęp do danych o zdarzeniach i ich automatyczne przetwarzanie, niemożność dodawania punktów wykrywania w infrastrukturze chmury oraz trudności w skutecznym kierowaniu zgłoszonych przez osoby trzecie nadużyć i incydentów z powrotem do właściwego odbiorcy lub dostawcy chmury w celu ich obsługi. Sytuacja różni się w zależności od modeli usług w chmurze i dostawców chmury [Gro10]. Na przykład dostawcy PaaS zazwyczaj nie udostępniają dzienników zdarzeń użytkownikom, którzy są wtedy zdani głównie na informacje o zdarzeniach z samodzielnie wdrożonych aplikacji (np. poprzez rejestry danych aplikacji). Podobnie, odbiorcy SaaS są całkowicie zależni od dostawcy chmury w zakresie dostarczania danych o zdarzeniach, takich jak rejestrowanie aktywności, podczas gdy odbiorcy IaaS kontrolują więcej ze stosu informacji i mają dostęp do powiązanych źródeł zdarzeń.
- **Analiza i rozwiązywanie incydentów.** Analiza mająca na celu potwierdzenie wystąpienia incydentu lub określenie metody jego przeprowadzenia musi być przeprowadzona szybko, z zachowaniem odpowiedniej szczegółowości dokumentacji i staranności, aby zapewnić zachowanie identyfikowalności i integralności do późniejszego wykorzystania w przypadku zaistnienia takiej potrzeby (np. kopia kryminalistyczna danych incydentu na potrzeby postępowania sądowego) [Gro10]. W celu uzyskania pełnego zrozumienia incydentu należy określić zakres zaatakowanych sieci, systemów i aplikacji; odkryć wektor włamania; oraz zrekonstruować przeprowadzone działania [Gro10]. Problemy, na które napotykają odbiorcy chmury podczas wykonywania analizy incydentu obejmują

brak szczegółowych informacji o architekturze chmury istotnej z punktu widzenia incydentu, brak informacji o powiązanych źródłach zdarzeń i danych posiadanych przez dostawcę chmury, źle zdefiniowane lub niejasne obowiązki związane z obsługą incydentu określone dla dostawcy chmury oraz ograniczone możliwości gromadzenia i zachowywania istotnych źródeł danych jako dowodów.

- Po określeniu zakresu incydentu i dotkniętych aktywów, można podjąć działania mające na celu opanowanie i rozwiązanie incydentu, przywracając systemy do bezpiecznego stanu operacyjnego [Gro10]. Role i obowiązki pomiędzy dostawcą i odbiorcą chmury w zakresie powstrzymywania ataku różnią się w zależności od modelu usług i architektury chmury. Na przykład w środowiskach SaaS i PaaS powstrzymywanie ataków polega zasadniczo na ograniczeniu lub usunięciu funkcjonalności (np. poprzez odfiltrowanie pewnych użytkowników lub funkcji za pomocą zapory aplikacji sieciowej), którą atakujący wykorzystuje do prowadzenia nieautoryzowanych działań, w razie potrzeby wyłączając całą aplikację z działania [Gro10]. W środowiskach chmurowych IaaS odbiorca chmury odgrywa bardziej znaczącą rolę, jednak pomoc dostawcy chmury jest niezbędna do usunięcia podatności wykorzystanych w bazowej infrastrukturze chmury

Reakcja na incydent powinna być prowadzona w sposób, który ogranicza szkody i minimalizuje czas i koszty odzyskiwania. Współpraca pomiędzy odbiorcą i dostawcą chmury w zakresie rozpoznawania i reagowania na incydent jest kluczowa dla bezpieczeństwa i ochrony prywatności w przetwarzaniu w chmurze. Przyporządkowane zgodnie z przepisami organizacje mają obowiązek zgłaszania pewnych kategorii incydentów do stosownego Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT) w ciągu określonego czasu od odkrycia lub wykrycia.[22] Potrzebne jest jasne zrozumienie rodzaju incydentów, które podlegają raportowaniu przez dostawcę usługi w chmurze (np. naruszenia danych) w porównaniu z tymi, które nie podlegają raportowaniu (np. alarmy wykrywające włamania). Środki

[22] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2018 r. poz. 1560)

zaradcze mogą angażować tylko jedną stronę lub wymagać udziału obu stron. Zdolność do szybkiego zwołania mieszanego zespołu przedstawicieli dostawcy i odbiorcy chmury jest ważnym aspektem skutecznej i efektywnej kosztowo reakcji.

Skuteczność działania zespołu reagowania na incydenty wymaga, aby był on w stanie działać autonomicznie i zdecydowanie. Rozwiązanie problemu może mieć wpływ na wielu odbiorców usługi w chmurze. Ważne jest, aby dostawcy usług w chmurze mieli przejrzysty proces reagowania oraz mechanizmy dzielenia się informacjami ze swoimi usługobiorcami w trakcie i po incydencie. Zrozumienie i wynegocjowanie postanowień i procedur dotyczących reagowania na incydenty powinno być dokonane przed zawarciem umowy o świadczenie usług, a nie po fakcie. Na przykład, plany reagowania na incydenty powinny uwzględniać naruszenia obejmujące informacje osobiste oraz sposoby minimalizowania ilości tych informacji podczas zgłaszania i reagowania na naruszenie [Mcc10]. Lokalizacja geograficzna danych jest powiązaną kwestią, która może utrudnić dochodzenie i jest istotnym przedmiotem negocjacji umowy.

4.10. PODSUMOWANIE ZALECEŃ

Szereg istotnych kwestii związanych z bezpieczeństwem i prywatnością zostało omówionych w poprzednich podrozdziałach. Tabela 2 podsumowuje te kwestie i związane z nimi zalecenia, którymi organizacje powinny się kierować podczas planowania, przeglądu, negocjowania lub inicjowania umowy outsourcingu usług w chmurze publicznej.

Tabela 2. Rekomendacje i wyzwania związane z bezpieczeństwem i ochroną prywatności.

Obszary	Zalecenia
Zarządzanie	Rozszerzenie praktyk organizacyjnych odnoszących się do polityk, procedur i standardów wykorzystywanych do rozwoju aplikacji i dostarczania usług w chmurze, a także projektowania, wdrażania, testowania, użytkowania i monitorowania wdrożonych lub zaangażowanych usług. Wdrożenie mechanizmów i narzędzi audytu w celu zapewnienia, że praktyki organizacyjne są przestrzegane w całym cyklu życia systemu.
Zgodność	Znajomość poszczególnych kategorii praw i regulacji, które nakładają na organizację obowiązki związane z bezpieczeństwem i ochroną prywatności oraz potencjalnie wpływają na inicjatywy przetwarzania w chmurze, w szczególności te, które dotyczą lokalizacji danych, zabezpieczeń prywatności i bezpieczeństwa, zarządzania rejestrami oraz wymogów związanych z elektronicznym ujawnianiem informacji. Przegląd i ocena ofert dostawcy usługi w chmurze w odniesieniu do wymogów organizacyjnych, które mają być spełnione oraz zapewnienie, że warunki umowy odpowiednio spełniają te wymogi. Upewnienie się, że możliwości i procesy elektronicznego odkrywania dostawcy chmury nie naruszają prywatności lub bezpieczeństwa danych i aplikacji.

Obszary	Zalecenia
Zaufanie	Zapewnienie, że umowy o świadczenie usług zawierają odpowiednie zapisy umożliwiające wgląd w środki i procesy bezpieczeństwa i ochrony prywatności stosowane przez dostawcę usługi w chmurze oraz ich skuteczność działania w czasie. Ustanowienie jasnych, wyłącznych praw własności do danych. Wprowadzenie programu zarządzania ryzykiem, który jest wystarczająco elastyczny, aby dostosować się do stale ewoluującego i zmieniającego się środowiska ryzyka w całym cyklu życia systemu. Stałe monitorowanie stanu bezpieczeństwa systemu informacyjnego w celu wspierania bieżących decyzji w zakresie zarządzania ryzykiem.
Architektura	Zrozumienie bazowych technologii, które dostawca usługi w chmurze wykorzystuje do świadczenia usług, w tym wpływu, jaki zaangażowane zabezpieczenia techniczne mają na bezpieczeństwo i ochronę prywatności w systemie, w całym cyklu życia systemu i we wszystkich komponentach systemu.
Zarządzanie tożsamością i dostępem	Zapewnienie, że istnieją odpowiednie środki bezpieczeństwa zapewniające uwierzytelnianie, autoryzację oraz inne funkcje zarządzania tożsamością i dostępem, a także, że są one dostosowane do potrzeb organizacji.
Izolacja oprogramowania	Zrozumienie wirtualizacji i innych technik logicznej izolacji, które dostawca chmury stosuje w swojej architekturze oprogramowania wielodostępowego, oraz ocena ponoszonego przez organizację ryzyka.
Ochrona danych	Ocena przydatności rozwiązań dostawcy chmury w zakresie zarządzania danymi mającymi znaczenie dla organizacji oraz zdolności do kontrolowania dostępu do danych, zabezpieczania danych w czasie spoczynku, w tranzycie i w użyciu oraz sanityzacji danych.

Obszary	Zalecenia
Dostępność	Zrozumienie postanowień umowy i procedur dotyczących dostępności, tworzenia kopii zapasowych i odzyskiwania danych oraz odtwarzania po awarii, a także zapewnienie, że spełniają one wymagania organizacji dotyczące ciągłości działania i planowania awaryjnego. Zapewnienie, że podczas czasowych lub długotrwałych zakłóceń lub poważnej awarii, krytyczne operacje mogą być natychmiast wznowione, oraz że wszystkie operacje mogą być ostatecznie przywrócone w sposób zorganizowany i terminowy.
Reakcja na incydenty	Zrozumienie zapisów umowy i procedur reagowania na incydenty i upewnienie się, że spełniają one wymagania organizacji. Zapewnienie, że dostawca usługi w chmurze posiada przejrzysty proces reagowania i wystarczające mechanizmy do dzielenia się informacjami w trakcie i po incydencie. Zapewnienie, że organizacja może reagować na incydenty w sposób skoordynowany z dostawcą chmury, zgodnie z ich odpowiednimi rolami i obowiązkami dotyczącymi środowiska przetwarzania.

5. PODWYKONAWSTWO W CHMURZE PUBLICZNEJ

Chociaż chmura obliczeniowa jest nowym paradygmatem obliczeniowym, to podwykonawstwo usług informatycznych już nim nie jest. Kroki, które podejmują organizacje pozostają zasadniczo takie same dla chmur publicznych, jak w przypadku innych, bardziej tradycyjnych usług informatycznych, a istniejące zalecenia dotyczące powierzania usług na zewnątrz również znajdują zastosowanie. To, co jednak zmienia się w przypadku chmury publicznej, to potencjalnie większa złożoność i trudność w zapewnieniu odpowiedniego nadzoru w celu zapewnienia rozliczalności i kontroli nad wdrożonymi aplikacjami i systemami w całym cyklu ich życia. Może to być szczególnie zniechęcające, jeśli warunki umowy o świadczenie usług nie spełniają w pełni potrzeb organizacji, ponieważ odpowiedzialność zazwyczaj ponoszona przez organizację jest przekazywana dostawcy usługi w chmurze, a bez wystarczających zapisów organizacja będzie miała niewielkie możliwości rozwiązywania problemów i rozstrzygania w sposób satysfakcjonujący kwestii, które mogą się pojawić. Oznacza to, że umowa o świadczenie usług jest podstawowym środkiem dla organizacji do egzekwowania zabezpieczeń i utrzymania odpowiedzialności za środowisko przetwarzania. Jeśli nie zostaną spełnione niezbędne wymagania lub poręczenia, odpowiedzialność za usługi jest tym samym zagrożona.

Historia tradycyjnego podwykonawstwa usług informatycznych jest zróżnicowana pod względem bezpieczeństwa i ochrony prywatności i nie zawsze jest realizowana poprawnie przez organizacje (np. [GAO06, GAO10]). Jak zostało to omówione w poprzednim rozdziale, przeniesieniu danych i funkcji organizacyjnych do chmury publicznej towarzyszy szereg kwestii bezpieczeństwa i ochrony prywatności, którymi należy się zająć, a wiele z nich dotyczy adekwatności zabezpieczeń technicznych dostawcy chmury do potrzeb organizacji. Ustalenia dotyczące usług określone w warunkach świadczenia usług muszą również spełniać politykę prywatności organizacji oraz obowiązujące przepisy prawa i regulacje dotyczące ochrony, rozpowszechniania i ujawniania informacji, do których organizacja musi się stosować. Każdy dostawca chmury i ustalenia dotyczące usług posiadają odmienne koszty

i ryzyka związane z tymi ustaleniami. Decyzja podjęta na podstawie jednej kwestii może mieć poważne implikacje dla organizacji w innych obszarach [Gra03].

Biorąc pod uwagę rosnącą liczbę dostawców chmury publicznej i szeroki zakres oferowanych przez nich usług, organizacje muszą zachować należytą staranność przy wyborze i przenoszeniu funkcjonalności do chmury publicznej. Podejmowanie decyzji o usługach i ustaleniach dotyczących usług wiąże się z osiągnięciem równowagi pomiędzy korzyściami w zakresie kosztów i produktywności, a negatywnymi skutkami w zakresie ryzyka i odpowiedzialności. Podczas gdy wrażliwość danych przetwarzanych przez organizacje publiczne oraz obecny stan techniki sprawiają, że prawdopodobieństwo powierzenia wszystkich usług informatycznych chmurze publicznej jest niskie, dla większości organizacji publicznych powinno być możliwe wdrożenie niektórych swoich usług informatycznych w chmurze publicznej, pod warunkiem, że podjęte zostaną wszystkie wymagane środki ograniczające ryzyko.

5.1. UWAGI OGÓLNE

Warunki klasycznych umów podwykonawczych z zakresu technologii informatycznych, szczególnie tych dotyczących danych wrażliwych, mogą służyć jako wytyczne dla inicjatyw przetwarzania w chmurze. Trzy główne kwestie związane z bezpieczeństwem i ochroną prywatności identyfikowane w umowach o świadczenie usług związanych z podwykonawstwem publicznych usług chmur obliczeniowych, to [All88, Len03]:

- **Nieadekwatne polityki i praktyki.** Polityki i praktyki bezpieczeństwa dostawcy chmury mogą nie być adekwatne lub kompatybilne z tymi, które obowiązują w organizacji. Ta sama kwestia dotyczy również ochrony prywatności. Może to skutkować wystąpieniem takich komplikacji jak [] All88]:
  - ✓ Niewykryte włamania lub naruszenia z powodu braku wystarczających polityk audytu i monitorowania przez dostawcę chmury;
  - ✓ Brak wystarczającej integralności danych i konfiguracji z powodu niedopasowania polityk organizacji i dostawcy chmury w zakresie rozdzielenia obowiązków (tj. jasnego przypisania ról i odpowiedzialności) lub redundancji (tj.

posiadania wystarczających mechanizmów kontroli i balansu) w celu zapewnienia, że operacja jest wykonywana konsekwentnie i prawidłowo;

- ✓ Utrata prywatności spowodowana tym, że dostawca chmury postępuje z wrażliwymi informacjami mniej rygorystycznie niż nakazuje to polityka organizacji.

- **Słabe gwarancje poufności i integralności.** Niewystarczające środki bezpieczeństwa stosowane na platformie dostawcy usługi w chmurze mogą negatywnie wpłynąć na poufność i prywatność lub integralność systemu. Na przykład, wykorzystanie niezabezpieczonej metody zdalnego dostępu może pozwolić intruzom na uzyskanie nieautoryzowanego dostępu, modyfikację lub zniszczenie systemów i zasobów informacyjnych organizacji; na celowe wprowadzenie do systemu luk w zabezpieczeniach lub złośliwego oprogramowania; lub na przeprowadzenie ataków na inne systemy z sieci organizacji, potencjalnie czyniąc organizację odpowiedzialną za poniesione szkody [All88].
- **Słabe gwarancje dostępności.** Niewystarczające zabezpieczenia zastosowane w platformie dostawcy chmury mogą negatywnie wpłynąć na dostępność systemu. Poza bezpośrednio dotkniętymi aplikacjami, utrata dostępności systemu może spowodować zagrożenie kluczowych zasobów, które są wymagane dla krytycznych operacji organizacyjnych. Na przykład, jeśli zakłócające operacje przetwarzania (np. równoważenie obciążenia z powodu usterki obiektu lub prac awaryjnych) są wykonywane przez dostawcę chmury w tym samym czasie, gdy występuje szczytowe przetwarzanie danych organizacji, może wystąpić stan odmowy usługi [All88]. Atak odmowy usługi skierowany na dostawcę chmury może również wpłynąć na aplikacje i systemy organizacji działające w chmurze lub w centrum danych organizacji.

Zapewnienia potwierdzające deklaracje bezpieczeństwa przekazane organizacji przez dostawcę usługi w chmurze lub przez podmiot zajmujący się przeglądem certyfikacji i zgodności finansowany przez dostawcę usługi w chmurze, powinny być zweryfikowane, gdy tylko jest to możliwe, poprzez niezależną ocenę organizacji.

Ponadto certyfikacja strony trzeciej lub inne zapewnienia ze strony dostawcy usługi w chmurze niekoniecznie przyznają aplikacji lub systemowi dzierżawcy ten sam poziom certyfikacji lub zgodności; te elementy prawdopodobnie wymagałyby oddzielnej oceny certyfikacji dla tego konkretnego środowiska w chmurze.[23]

Inne godne uwagi obawy, które są pośrednio związane z bezpieczeństwem i ochroną prywatności, również istnieją w przypadku powierzania przetwarzania danych w chmurach publicznych. Jeden z najbardziej powszechnych i wyzywających problemów jest nazywany problemem zleceniodawcy-agenta. Kolejnym jest osłabienie technicznej wiedzy eksperckiej organizacji.

- **Problem zleceniodawca-agent**. Problem relacji zleceniodawca-agent występuje, gdy motywacje agenta (tj. dostawcy usługi w chmurze) nie są zgodne z interesami zleceniodawcy (tj. organizacji) [Row07]. Ponieważ może być trudno określić poziom wysiłku, jaki dostawca usługi w chmurze wkłada w administrowanie bezpieczeństwem i ochroną prywatności oraz remediację, istnieje obawa, że organizacja może nie rozpoznać, czy poziom usług spada lub spadł poniżej wymaganego zakresu. Jednym z utrudnień jest to, że zwiększone wysiłki w zakresie bezpieczeństwa nie gwarantują rezultatu w postaci zauważalnej poprawy (np. mniejszej liczby incydentów), częściowo z powodu rosnącej ilości złośliwego oprogramowania i nowych rodzajów ataków [Row07].
- **Spadek poziomu wiedzy specjalistycznej**. Usługi obliczeniowe zlecane na zewnątrz mogą z czasem zmniejszyć poziom wiedzy technicznej i doświadczenia organizacji, ponieważ kierownictwo i personel nie muszą już regularnie zajmować się kwestiami technicznymi na szczegółowym poziomie [Gon09]. W miarę jak nowe postępy i ulepszenia są wprowadzane do środowiska chmury obliczeniowej, zdobyta wiedza i doświadczenie przynoszą bezpośrednie korzyści dostawcy chmury, a nie

[23] Federalny Program Zarządzania Ryzykiem i Autoryzacją został ustanowiony w celu zapewnienia standardowego podejścia do oceny i autoryzacji usług i produktów chmury obliczeniowej, które skutkuje wspólną autoryzacją dostawców chmury w odniesieniu do wspólnego modelu ryzyka bezpieczeństwa. Wydana wspólna autoryzacja może być ponownie użyta i wykorzystana we wdrożeniach przetwarzania w chmurze w organizacjach, do których stosuje się model ryzyka bezpieczeństwa - http://www.cio.gov/modules/fedramp/demo.cfm.

organizacji. Jeżeli nie zostaną podjęte środki ostrożności, organizacja może stracić zdolność do nadążania za postępem technologicznym oraz powiązanymi względami bezpieczeństwa i ochrony prywatności, co z kolei może wpłynąć na jej zdolność do efektywnego planowania i nadzorowania nowych projektów informatycznych oraz do utrzymania odpowiedzialności za istniejące systemy oparte na chmurze.

Organizacja może być w stanie zastosować kompensujące środki bezpieczeństwa i ochrony prywatności, pozwalające na ominięcie zidentyfikowanych niedociągnięć w usłudze chmury publicznej. Nienegocjowane umowy o świadczenie usług generalnie ograniczają zakres dostępnych dla organizacji działań ograniczających ryzyko, podczas gdy negocjowane umowy o świadczenie usług, które zapewniają większy zakres i elastyczność, wymagają starannej analizy i priorytetyzacji wymogów, które są włączone do warunków świadczenia usług, tak, aby była ona efektywna kosztowo. W każdym z tych przypadków jest jednak mało prawdopodobne, aby dostępne techniki ograniczania ryzyka były kiedykolwiek wystarczające, aby pozwolić na rozmieszczenie w chmurze publicznej danych o wysokiej wartości lub bardzo wrażliwych danych lub aplikacji o znaczeniu krytycznym. W takich sytuacjach organizacja może rozważyć zastosowanie środowiska przetwarzania w chmurze z bardziej odpowiednim modelem wdrożenia, takim jak wewnętrzna chmura prywatna, która może potencjalnie zapewnić większy nadzór i uprawnienia w zakresie bezpieczeństwa i ochrony prywatności oraz lepiej ograniczyć typy dzierżawców, którzy współdzielą zasoby platformy, zmniejszając ekspozycję w przypadku awarii lub błędu konfiguracji zabezpieczeń.

Istnieje kilka odrębnych etapów procesu podwykonawstwa, na których organizacja może przeprowadzić określone działania, aby utrzymać rozliczalność i złagodzić wyżej wymienione kwestie związane z bezpieczeństwem i ochroną prywatności: podczas planowania działań ("działania wstępne"), podczas inicjowania kontraktu na usługi i nadzorowania go ("działania początkowe i towarzyszące") oraz podczas zamykania usług i kontraktu ("działania końcowe") [All88, Len03]. W kolejnych częściach tego rozdziału szczegółowo omówiono te etapy.

Narodowe Standardy Bezpieczeństwa (NSC) odnoszą się do wszystkich etapów podwykonawstwa, w szczególności NSC199 i NSC 200, które dotyczą planowania we wczesnych etapach.

- **NSC 199.** Standard ten, zatytułowany *Standardy kategoryzacji bezpieczeństwa*, stanowi wspólne ramy i metodę kategoryzacji informacji i systemów informacyjnych w celu zapewnienia odpowiedniego poziomu bezpieczeństwa informacji, współmiernego do poziomu ryzyka. Wynikająca z tego kategoryzacja bezpieczeństwa jest podstawą do innych działań, takich jak wybór środków bezpieczeństwa, analiza wpływu na prywatność oraz analiza infrastruktury krytycznej.
- **NSC 200.** Standard ten, zatytułowany *Minimalne wymogi bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych*, zobowiązuje organizacje do spełnienia określonych minimalnych wymogów bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych poprzez wybór odpowiednich środków bezpieczeństwa i wymogów dotyczących wiarygodności opisanych w standardzie NSC 800-53 wer. 2.

Informacje i wskazówki na temat planowania, wdrażania i zarządzania bezpieczeństwem systemów informacyjnych oraz ochrony informacji, które mają zastosowanie do inicjatyw związanych z podwykonawstwem w środowiskach przetwarzania w chmurze, są zawarte dokumentach przedstawionych w Tabeli 3 i powinny być stosowane w połączeniu z tą publikacją.[24]

[24] Informacje na temat tych wytycznych NIST, jak również innych publikacji związanych z bezpieczeństwem, można znaleźć na stronie internetowej NIST - http://csrc.nist.gov/publications/index.html.

Tabela 3. Wybrane Narodowe Standardy Cyberbezpieczeństwa (NSC) oraz Publikacje Specjalne NIST (NIST SP).

Publikacja	Tytuł
NSC 800-18	Przewodnik do opracowywania planów bezpieczeństwa systemów informacyjnych w podmiotach publicznych – na podstawie NIST SP 800 18
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 w systemach informacyjnych oraz organizacjach – na podstawie NIST SP 800-53
NSC 800-53A	Ocenianie środków bezpieczeństwa i ochrony prywatności w systemach informacyjnych oraz organizacjach. 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
NIST SP 800-64	Security Considerations in the System Development Life Cycle
NIST SP 800-86	Guide to Integrating Forensic Techniques into Incident Response
NIST SP 800-88	Guidelines for Media Sanitization
NIST SP 800-115	Technical Guide to Information Security Testing and Assessment
NIST SP 800-122	Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
NIST SP 800-137	Information Security Continuous Monitoring for Federal Information Systems and Organizations

Istnieje możliwość elastycznego stosowania tych wytycznych przez organizacje. Powinny one stosować koncepcje i zasady bezpieczeństwa wyartykułowane w specjalnych publikacjach NSC zgodnie z misją, funkcjami biznesowymi i środowiskiem działania danej organizacji oraz w ich kontekście. W związku z tym stosowanie wytycznych NSC przez organizacje może skutkować różnymi rozwiązaniami w zakresie bezpieczeństwa, które są akceptowalne zgodne z wytycznymi i spełniają definicję dotyczącą odpowiedniego bezpieczeństwa systemów informacyjnych organizacji.

5.2. DZIAŁANIA PRZYGOTOWAWCZE

W pierwszym etapie procesu zlecania usług na zewnątrz organizacja musi wykonać określone czynności planistyczne w ramach przygotowań do zawarcia umowy na usługi w chmurze publicznej. Planowanie pomaga zapewnić, że organizacja czerpie pełne korzyści z nakładów poniesionych na technologie informatyczne. Pomaga również zapewnić, że środowisko obliczeniowe jest tak bezpieczne, jak to tylko możliwe i zgodne ze wszystkimi odpowiednimi politykami organizacji oraz, że zachowana jest prywatność danych. Działania związane z planowaniem obejmują następujące elementy:

- **Określenie wymagań.** Organizacja jest zobowiązana określić swoje wymagania dotyczące bezpieczeństwa, ochrony prywatności i inne wymogi dotyczące usług w chmurze, jako kryterium wyboru dostawcy chmury. Typowe wymagania dotyczące bezpieczeństwa obejmują uwzględnienie następujących obszarów [CSA11b, Len03]:
  - ✓ Wymogi dotyczące personelu, w tym poświadczenia bezpieczeństwa, role i obowiązki.
  - ✓ Wymogi regulacyjne.
  - ✓ Dostępność usługi.
  - ✓ Sprawozdawczość, przegląd i rozwiązywanie problemów.
  - ✓ Umowy i procedury dotyczące przetwarzania i ujawniania informacji.

- ✓ Fizyczne i logiczne zabezpieczenia dostępu.
- ✓ Kontrola dostępu do sieci, łączności i filtrowania.
- ✓ Ochrona danych.
- ✓ Konfiguracja systemu i zarządzanie poprawkami.
- ✓ Tworzenie kopii zapasowych i odzyskiwanie danych.
- ✓ Przechowywanie danych i sanityzacja.
- ✓ Skanowanie bezpieczeństwa i podatności na zagrożenia.
- ✓ Zarządzanie ryzykiem.
- ✓ Zgłaszanie, obsługa i reagowanie na incydenty.
- ✓ Ciągłość działania.
- ✓ Zarządzanie zasobami.
- ✓ Certyfikacja i akredytacja.
- ✓ Poziomy wiarygodności.
- ✓ Niezależny audyt usług.

Część analizy wymagań powinna zawęzić wybór pomiędzy modelami usług IaaS, PaaS i SaaS do jednego wyboru, który jest dostosowany do konkretnych potrzeb i celów organizacji. Obowiązki zarówno organizacji jak i dostawcy chmury różnią się w zależności od modelu usługi. Na przykład w IaaS odpowiedzialność dostawcy chmury zazwyczaj kończy się na hiperwizorze. Organizacje korzystające z usług w chmurze muszą rozumieć rozgraniczenie odpowiedzialności i to, w jaki sposób muszą one być powiązane z procesami dostawcy chmury, aby zapewnić, że praktyki ładu organizacyjnego są rozszerzone na to środowisko oraz że zapewnione są mechanizmy i narzędzia do zarządzania tymi aspektami, które są w zakresie odpowiedzialności organizacji.

Ustanowienie strategii wyjścia jest ważną częścią procesu planowania i powinno być uwzględnione w analizie wymagań. Odnosi się to również do działań organizacji w zakresie planowania awaryjnego i ciągłości działania. Strategia wyjścia powinna

obejmować zarówno standardowe wypowiedzenie, takie jak wygaśnięcie umowy o świadczenie usług, jak i nieprzewidziane wypowiedzenie, np. z powodu bankructwa dostawcy usług lub słabych parametrów [Gra03]. Zdolność do wyeksportowania wszystkich danych organizacji w użytecznym formacie za pomocą bezpiecznych, niezawodnych i wydajnych środków oraz w odpowiednim czasie, jest istotnym aspektem strategii wyjścia. Inne aspekty obejmują zaadresowanie zależności aplikacji od własnościowych interfejsów programowania, wywołań systemowych i technologii baz danych, a także odzyskanie użytecznych metadanych, które mogły zostać zgromadzone w środowisku chmury.

Zgodność z różnymi standardami, wytycznymi i przepisami prawnymi narzuca wymagania, które muszą być uwzględnione w analizie wymagań. Implikacje niektórych kluczowych praw i regulacji zostały omówione w poprzednim rozdziale, niemniej istnieją także inne. Wymagania związane ze zgodnością, takie jak ochrona danych osobowych, mogą być również specyficzne dla danej organizacji [Mcc10]. Istnieją również inne wymagania związane z podwykonawstwem, takie jak kontrola zarządzania dokumentacją, dostępność i szkolenie użytkowników, które również należy uwzględnić.

Przegląd powszechnych postanowień o powierzeniu świadczenia usług w obowiązujących umowach przetwarzania w chmurze, które obejmują takie obszary jak standardy prywatności i bezpieczeństwa, kwestie regulacyjne i zgodności, kryteria i kary za zapewnienie poziomu usług, procesy zarządzania zmianami, postanowienia dotyczące ciągłości usług oraz prawa do wypowiedzenia, mogą być pomocne w formułowaniu wymagań [Ove10]. Użyteczne mogą być również istniejące umowy o korzystanie z zewnętrznych usług informatycznych stosowane przez organizację.

Zasady Uczciwych Praktyk Informacyjnych. Uczciwe Praktyki Informacyjne, znane również jako Zasady Ochrony Prywatności, stanowią ramy większości nowoczesnych przepisów dotyczących ochrony prywatności na świecie [Mcc10]. Organizacja Współpracy Gospodarczej i Rozwoju (OECD), przyjęła w 1980 r. Wytyczne w sprawie ochrony prywatności i transgranicznego przepływu danych osobowych [OECD80]. Wytyczne te stanowią ramy dla prywatności, do których odwołują się amerykańskie

wytyczne federalne, a także międzynarodowe, i mogą być wykorzystywane przez agencje federalne do formułowania swoich wymagań i uwzględniania problemów związanych z prywatnością podczas planowania. Wytyczne określają osiem następujących zasad ochrony prywatności:

- *Ograniczenie gromadzenia danych*. Gromadzenie danych osobowych powinno być ograniczone, a wszelkie takie dane powinny być uzyskiwane w sposób zgodny z prawem i uczciwy oraz, w stosownych przypadkach, za wiedzą lub zgodą osoby, której dane dotyczą.
- *Jakość danych*. Dane osobowe powinny odpowiadać celom, do których mają być użyte oraz, w zakresie niezbędnym do tych celów, powinny być dokładne, kompletne i aktualne.
- *Określenie celu*. Cele, dla których gromadzone są dane osobowe, powinny być określone najpóźniej w momencie gromadzenia danych, a ich dalsze wykorzystanie powinno być ograniczone do realizacji tych celów lub innych, które nie są sprzeczne z tymi celami i które są określane przy każdej zmianie celu.
- *Ograniczanie wykorzystania*. Dane osobowe nie powinny być ujawniane, udostępniane ani w inny sposób wykorzystywane do celów innych niż te, które zostały określone zgodnie z poprzednią zasadą, chyba, że: za zgodą osoby, której dane dotyczą; lub na mocy prawa.
- *Środki bezpieczeństwa*. Dane osobowe powinny być chronione za pomocą stosownych zabezpieczeń przed utratą lub nieuprawnionym dostępem, zniszczeniem, wykorzystaniem, modyfikacją lub ujawnieniem ich zawartości.
- *Przejrzystość*. Powinna istnieć ogólna polityka przejrzystości w odniesieniu do rozwoju, praktyk i polityk dotyczących danych osobowych. Powinny być łatwo dostępne środki pozwalające ustalić istnienie i charakter danych osobowych oraz główne cele ich wykorzystania, jak również tożsamość i miejsce stałej rezydencji administratora danych.
- *Uczestnictwo indywidualne*. Osoba fizyczna powinna mieć prawo:

a) uzyskania od administratora danych (lub w inny sposób) potwierdzenia, czy administrator danych przetwarza dane jej dotyczące;

b) otrzymania informacji o tym, że dane jej dotyczące zostały jej przekazane w stosownym terminie;

c) otrzymania uzasadnienia, jeżeli wniosek złożony zgodnie z lit. a) i b) zostanie odrzucony, oraz możliwości zakwestionowania takiej odmowy; oraz

d) zakwestionowania danych, które jej dotyczą, a jeżeli zakwestionowanie okaże się skuteczne - usunięcia, poprawienia, uzupełnienia lub zmiany tych danych.

- *Rozliczal*ność. Administrator danych powinien być odpowiedzialny za przestrzeganie środków, które zapewniają skuteczność wyżej wymienionych zasad.

Pięć podstawowych zasad ochrony prywatności zawarto również w kodeksie rzetelnej praktyki informacyjnej (*ang. Fair Information Practice Codes*) [FTC07]. Są one podobne do tych zawartych w wytycznych OECD, ale skierowane do podmiotów komercyjnych. Niemniej jednak, zasady te zapewniają użyteczną, uzupełniającą perspektywę ochrony prywatności.

- *Zawiadomienie/ogłoszenie*. Konsumenci powinni być informowani o praktykach informacyjnych podmiotu przed zebraniem jakichkolwiek danych osobowych, aby umożliwić podjęcie świadomej decyzji o zakresie, jeżeli takowy istnieje, ujawnienia danych osobowych. Zawiadomienie o niektórych lub wszystkich następujących elementach uważa się za istotne dla zapewnienia, że konsumenci są właściwie poinformowani: identyfikacja podmiotu gromadzącego dane; identyfikacja sposobów wykorzystania danych; identyfikacja wszelkich potencjalnych odbiorców danych; charakter gromadzonych danych oraz sposoby ich gromadzenia, jeżeli nie są one oczywistością (np. biernie, za pomocą elektronicznego monitoringu, lub czynnie, prosząc konsumenta o dostarczenie informacji); wskazanie, czy podanie żądanych danych jest dobrowolne czy wymagane, oraz konsekwencje odmowy podania żądanych informacji; oraz kroki podjęte w celu zapewnienia poufności, integralności i jakości zebranych danych.

- *Wybór/zgoda*. Wybór oznacza danie konsumentowi możliwości wyboru sposobu wykorzystania zebranych danych osobowych. Wybór odnosi się w szczególności do wtórnego wykorzystania informacji, które wykracza poza to, co jest potrzebne do przeprowadzenia planowanej transakcji. Dwa główne rodzaje systemów wyboru/zgody to „opt-in" lub „opt-out". Pierwszy z nich wymaga potwierdzenia przez konsumenta, aby zezwolić na zbieranie danych, natomiast drugi wymaga potwierdzenia, aby temu zapobiec. Wybór może również obejmować więcej niż opcję binarną i umożliwiać konsumentom dostosowanie rodzaju ujawnianych przez nich informacji oraz dopuszczalnych sposobów ich wykorzystania.
- *Dostęp/uczestniczenie*. Dostęp odnosi się do zdolności jednostki do przeglądania przechowywanych danych dotyczących jej osoby oraz do kwestionowania dokładności i kompletności tych danych. Proces ten powinien być prosty, terminowy i niewymagający nakładów finansowych ze strony konsumenta, a także powinien umożliwiać uwzględnienie sprzeciwu konsumenta i przesłanie go do odbiorców danych.
- *Integralność/bezpieczeństwo*. Integralność wymaga, aby dane były prawdziwe i bezpieczne. Aby zapewnić integralność, należy zastosować odpowiednie środki, np. porównywanie danych z wieloma źródłami w celu sprawdzenia ich dokładności. Bezpieczeństwo obejmuje środki ochrony przed utratą i nieuprawnionym dostępem, zniszczeniem, wykorzystaniem, modyfikacją i ujawnieniem danych.
- *Egzekwowanie/odszkodowanie*. Ochrona prywatności może być skuteczna tylko wtedy, gdy istnieje mechanizm egzekwowania podstawowych zasad i zaradzania niepożądanym lub nieuczciwym sytuacjom związanym z gromadzonymi danymi. Administrator danych, na rzecz którego odbywa się przetwarzanie danych, powinien być odpowiedzialny za przestrzeganie podstawowych zasad. Możliwością dochodzenia roszczeń jest egzekwowanie przepisów poprzez samoregulację branży, przepisy umożliwiające konsumentom korzystanie z prywatnych środków ochrony prawnej oraz systemy regulacyjne egzekwowane poprzez sankcje cywilne i karne.

- **Ocena zagrożeń dla bezpieczeństwa i prywatności.** Podczas gdy korzystanie z podwykonawców zmniejsza zaangażowanie operacyjne ze strony organizacji, zaangażowanie usług chmury publicznej wiąże się z ryzykiem, przed którym organizacja musi się zabezpieczyć. W poprzednim rozdziale podkreślono znaczenie ustanowienia elastycznego i adaptowalnego programu zarządzania ryzykiem w cyklu życia systemu. Analiza ryzyka przeprowadzona na tym etapie powinna obejmować czynniki takie jak zastosowany model usługi, cel i zakres usługi, rodzaje i poziom dostępu wymaganego przez dostawcę i proponowanego do wykorzystania pomiędzy środowiskiem obliczeniowym organizacji, a usługami dostawcy, czas trwania usługi i ich zależności oraz siłę ochrony oferowanej poprzez mechanizmy bezpieczeństwa udostępniane przez dostawcę chmury [Len03]. Inną kwestią, jeżeli ma zastosowanie nienegocjowana umowa o świadczenie usług, jest to, czy warunki usługi podlegają jednostronnej zmianie przez dostawcę usługi w chmurze, co mogłoby zwiększyć ryzyko związane z bezpieczeństwem i ochroną prywatności [CIO10a]. Zabezpieczenia prywatności powinny być oceniane jako część analizy, podobnie jak ryzyka operacyjne wynikające z lokalizacji obiektów dostawcy usługi w chmurze.

  Organizacja może wymagać, aby analiza progu ochrony prywatności (*ang. Privacy Threshold Analysis - PTA*) została zakończona przed opracowaniem lub nabyciem nowego systemu informacyjnego oraz gdy w istniejącym systemie dokonywana jest istotna zmiana [Mcc10]. PTA są wykorzystywane do określenia, czy system zawiera dane osobowe, czy wymagana jest ocena wpływu na prywatność (*ang. Privacy Impact Assessment - PIA*) lub system ewidencji informacji (*ang. System of Records Notice - SORN*[25]) oraz czy do systemu informacyjnego mają zastosowanie inne wymagania dotyczące prywatności. Jak wspomniano wcześniej, PIA jest zwykle przeprowadzana dla wszystkich nowych lub znacznie zmienionych technologii, które gromadzą, przechowują lub rozpowszechniają dane osobowe i udostępniają je publicznie.

[25] Oficjalna publiczna informacja o systemie(-ach) rejestrów organizacji, która określa: (i) cel systemu rejestrów; (ii) osoby objęte przez system rejestrów; (iii) kategorie rejestrów utrzymywanych na temat osób; oraz (iv) sposoby, w jakie informacje są udostępniane.

Dane osobowe powinny być oceniane w celu określenia potencjalnej szkody, jaka mogłaby wyniknąć dla osób i/lub organizacji, gdyby zostały niewłaściwie udostępnione, wykorzystane lub ujawnione (tj. ich poziom wpływu na poufność) [Mcc10]. Organizacja decyduje o czynnikach, które wykorzystuje do określania poziomów wpływu na poufność danych osobowych, a następnie tworzy i wdraża odpowiednią politykę, procedury i zabezpieczenia w celu ochrony informacji. Na przykład niektóre organizacje są prawnie zobowiązane do ochrony określonych rodzajów informacji osobistej i powinny uwzględnić te zobowiązania przy określaniu poziomów wpływu na poufność tych informacji i stosowaniu odpowiednich zabezpieczeń.[26]

Wrażliwość innych rodzajów danych przechowywanych przez organizację jest również istotnym czynnikiem przy analizie ryzyka.[27] Zakres danych, z którymi ma do czynienia organizacja, niekiedy nie jest w pełni doceniany. Podczas gdy repozytoria danych zawierające informacje prywatne lub niejawne są łatwiejsze do rozpoznania i uwzględnienia, mogą istnieć również inne rodzaje danych wrażliwych, z którymi wiążą się różne zasady postępowania. Należą do nich takie dane, jak np.:

- ✓ Dane organów ścigania i dochodzeniowych.
- ✓ Informacje dotyczące bezpieczeństwa systemu, takie jak schematy sieci, ustawienia konfiguracyjne i raporty o podatnościach na zagrożenia.
- ✓ Licencjonowany kod źródłowy i biblioteki używane przy tworzeniu aplikacji.
- ✓ Dokumenty i materiały cyfrowe uzyskane na podstawie umowy o zachowaniu poufności lub protokołu ustaleń.
- ✓ Dane laboratoryjne i badawcze, których gromadzenie, przechowywanie i udostępnianie podlegają regulacjom prawnym.

[26] Informacje na temat określania poziomów wpływu na poufność danych osobowych można znaleźć w dokumencie NIST SP 800-122, *Guide to Protecting Confidentiality of Personally Identifiable Information* - http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf.

[27] Wrażliwość danych pochodzących z innych organizacji może również stanowić istotny aspekt, jeśli są one skorelowane z danymi organizacyjnymi.

Zrozumienie podstawowych technologii, które dostawca chmury wykorzystuje do świadczenia usług, jest niezbędne do przeprowadzenia dokładnej analizy ryzyka. Kwestie bezpieczeństwa i ochrony prywatności omówione w poprzednim rozdziale wskazują ważne obszary technologii, które należy poddać przeglądowi:

- ✓ Techniki izolacji logicznej stosowane w architekturze oprogramowania wielodostępowego w chmurze.
- ✓ Rozwiązania do tworzenia kopii zapasowych i odzyskiwania danych oraz do sanityzacji danych.
- ✓ Funkcje i procesy elektronicznego odkrywania danych.
- ✓ Mechanizmy stosowane do kontroli dostępu do danych, do ochrony danych w stanie spoczynku, w tranzycie i w użyciu oraz do usuwania danych, gdy nie są już niezbędne.
- ✓ Dostępne urządzenia do zarządzania kryptografią i kluczami kryptograficznymi;
- ✓ Mechanizmy bezpiecznego uwierzytelniania, autoryzacji oraz inne funkcje zarządzania tożsamością i dostępem.
- ✓ Instrumenty do reagowania na incydenty i odzyskiwania danych po awarii.

Jak wspomniano wcześniej, jeżeli wyniki analizy ryzyka wykażą, że poziom ten jest zbyt wysoki, organizacja może być w stanie zastosować zabezpieczenia kompensacyjne, pozwalające na zmniejszenie ryzyka do akceptowalnego poziomu. W przeciwnym razie musi albo odrzucić wykorzystanie usługi, albo zaakceptować większy stopień ryzyka. Alternatywą dla wycofania się z usługi i rezygnacji z dalszych działań może być ograniczenie zakresu podwykonawstwa tak, aby obejmowało ono wyłącznie mniej wrażliwe dane. Podczas oceny ryzyka może również okazać się, że dla analizowanego modelu usługi i aplikacji inny model wdrożenia byłby bardziej odpowiedni niż chmura publiczna.

- **Ocena kompetencji dostawcy chmury.** Przed zawarciem umowy na świadczenie usług podwykonawczych, organizacja powinna ocenić zdolność i zobowiązanie

dostawcy usługi w chmurze do świadczenia usług w wyznaczonych ramach czasowych oraz spełnienia określonych poziomów bezpieczeństwa i ochrony prywatności. Dostawca chmury może zostać wezwany do zademonstrowania swoich kompetencji i podejścia do egzekwowania bezpieczeństwa i ochrony prywatności lub do poddania się niezależnej ocenie posiadanych instalacji i systemów [All88]. Kontaktowanie się z aktualnymi odbiorcami usług dostawcy usługi w chmurze, albo zidentyfikowanymi niezależnie (np. inne organizacje publiczne) bądź dostarczonymi przez dostawcę usługi w chmurze referencjami, oraz ocena poziomu ich satysfakcji w obszarach bezpieczeństwa i ochrony prywatności, które są przedmiotem zainteresowania organizacji, może również zapewnić wgląd w kompetencje dostawcy usługi w chmurze. Oprócz dokładnej oceny poziomów ochrony prywatności i bezpieczeństwa usług, które mają być świadczone, należy zwrócić uwagę na następujące elementy [Len03]:

- ✓ Doświadczenie i techniczna wiedza fachowa personelu.
- ✓ Proces weryfikacji, któremu poddawany jest personel.
- ✓ Jakość i częstotliwość szkoleń dotyczących świadomości w zakresie bezpieczeństwa i ochrony prywatności, jakie przeszedł personel.
- ✓ Praktyki zarządzania relacjami z klientami i odpowiedzialność za nie.
- ✓ Rodzaj i skuteczność świadczonych usług bezpieczeństwa oraz stosowane mechanizmy bazowe.
- ✓ Wskaźnik wdrażania nowych technologii.
- ✓ Procedury i procesy zarządzania modyfikacjami.
- ✓ Dotychczasowe doświadczenie dostawcy chmury.
- ✓ Zdolność dostawcy usługi w chmurze do spełnienia polityki bezpieczeństwa i ochrony prywatności organizacji, procedur i potrzeb w zakresie zgodności z przepisami.

5.3. DZIAŁANIA INICJUJĄCE I WSPÓŁBIEŻNE

Organizacja ma szereg czynności do przeprowadzenia w drugim etapie podwykonawczym, przyznając dostawcy chmury prawo do kontraktu i nadzorując warunki umowy przez cały okres jej trwania.

- **Ustalenie zobowiązań umownych.** Organizacja powinna zapewnić, że wszystkie wymagania umowne są wyraźnie określone w umowie o świadczenie usług, w tym postanowienia dotyczące ochrony prywatności i bezpieczeństwa [Gra03, Len03]. Umowa powinna zawierać definicje ról i obowiązków zarówno organizacji, jak i dostawcy usługi w chmurze. Organizacja powinna również upewnić się, że wszelkie zabezpieczenia kompensacyjne, których wymaga w celu zredukowania ryzyka do akceptowalnego poziomu, mogą być przeprowadzone w ramach warunków umowy. Warunki umowy powinny również obejmować następujące elementy [Gra03]:
  - ✓ Szczegółowy opis środowiska usług, w tym lokalizacji obiektów i obowiązujących wymogów bezpieczeństwa.
  - ✓ Polityki, procedury i normy, w tym weryfikacja i zarządzanie personelem.
  - ✓ Określone z góry poziomy usług i powiązane koszty.
  - ✓ Proces oceny zgodności usług dostawcy w chmurze z postanowieniami umowy SLA, w tym niezależne audyty i testy.
  - ✓ Określone środki zaradcze w przypadku wyrządzenia szkody lub nieprzestrzegania przez dostawcę usługi w chmurze.
  - ✓ Okres realizacji i terminy wymagalności dla wszelkich dostarczanych usług.
  - ✓ Punkty styku interfejsów dostawcy usługi w chmurze z organizacją.
  - ✓ Obowiązki organizacji w zakresie dostarczania dostawcy usługi w chmurze istotnych informacji i zasobów.
  - ✓ Procedury, zabezpieczenia i ograniczenia dotyczące kolokacji lub łączenia danych organizacji oraz przetwarzania wrażliwych danych.

- ✓ Obowiązki dostawcy usługi w chmurze po zakończeniu umowy, takie jak zwrot i usunięcie danych organizacyjnych.

W poprzednim rozdziale wskazano dodatkowe obszary, w których organizacja jest szczególnie zależna od dostawcy usług i w których warunki umowy o świadczenie usług powinny być wyjątkowo jasne, aby uniknąć potencjalnych problemów. Należą do nich między innymi następujące elementy:

- ✓ Prawa własności do danych.
- ✓ Lokalizacja danych organizacyjnych w środowisku chmury.
- ✓ Przejrzystość działania w zakresie bezpieczeństwa i ochrony prywatności.
- ✓ Dostępność usług i rozwiązania awaryjne.
- ✓ Tworzenie kopii zapasowych i odzyskiwanie danych.
- ✓ Koordynacja reakcji na incydenty i dzielenie się informacjami.
- ✓ Odtwarzanie awaryjne.

Przepisy dotyczące ochrony prywatności mogą być interpretowane inaczej przez osoby odpowiedzialne w organizacji za kwestie prawne i ochronę prywatności niż przez dostawcę usługi w chmurze. Organizacja musi dołożyć należytej staranności podczas przeglądu zabezpieczeń zapewnianych lub wynegocjowanych w umowie o świadczenie usług zawartej z dostawcą chmury, aby zidentyfikować i rozwiązać niespójności pomiędzy politykami prywatności organizacji i dostawcy chmury. Organizacje muszą zapewnić, że zapewnione zabezpieczenia są odpowiednie do ochrony danych rodzajów informacji planowanych do wdrożenia do środowiska chmury.

Przed zawarciem umowy wskazane jest, aby doświadczony doradca prawny dokonał szczegółowego przeglądu jej warunków. Nienegocjowane umowy o świadczenie usług są zazwyczaj sporządzane na korzyść dostawcy usługi w chmurze i mogą okazać się nie do zastosowania przez organizację.

- **Ocena wydajności.** Ciągła ocena działania dostawcy usługi w chmurze oraz jakości świadczonych usług jest niezbędna do zapewnienia, że wszystkie zobowiązania

umowne oraz wymagania organizacyjne są spełniane oraz jest istotną częścią procesu zarządzania ryzykiem.[28] Organizacja powinna analizować stan systemu regularnie i tak często, jak to jest konieczne, aby właściwie zarządzać ryzykiem związanym z bezpieczeństwem i ochroną prywatności. Ciągła ocena pozwala organizacji na podjęcie natychmiastowych działań korygujących lub karnych w przypadku zauważonych niedociągnięć, a także stanowi punkt odniesienia lub wzorzec do poprawy warunków umowy o świadczenie usług [All88, Gra03, Len03].

5.4. CZYNNOŚCI KOŃCOWE

Po zakończeniu projektu, przy przejściu do innego dostawcy chmury, lub z powodu innych przyczyn, organizacja może zdecydować się na zakończenie ostatniego etapu podwykonawstwa i zakończyć korzystanie z usług chmury publicznej oraz rozwiązać umowę. Organizacje powinny wykonać następujące czynności poprzedzające wypowiedzenie umowy podwykonawczej:

- **Potwierdzenie zobowiązań umownych.** Organizacja powinna powiadomić dostawcę usługi w chmurze o wszelkich istotnych wymogach umownych, które muszą być przestrzegane po zakończeniu, takich jak nieujawnianie pewnych warunków umowy oraz sanityzacja danych organizacyjnych z nośników [Len03].
- **Wyeliminowanie fizycznych i elektronicznych praw dostępu.** Jeżeli jakiekolwiek konta i prawa dostępu do zasobów obliczeniowych organizacji zostały przypisane dostawcy chmury w ramach umowy o świadczenie usług, powinny być one w odpowiednim czasie odwołane przez organizację [All88, Len03]. Podobnie, fizyczne prawa dostępu do tokenów i identyfikatorów bezpieczeństwa wydanych dostawcy chmury również muszą zostać odwołane, a wszelkie osobiste tokeny i identyfikatory używane do dostępu muszą zostać odzyskane [All88].

[28] Więcej informacji na temat ciągłości monitorowania i zarządzania ryzykiem można znaleźć w dokumencie NIST SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations oraz SP 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems - http://csrc.nist.gov/publications/index.html.

- **Odzyskanie zasobów i danych organizacji.** Organizacja powinna zapewnić, aby wszelkie zasoby organizacji udostępnione dostawcy usługi w chmurze na warunkach umowy o świadczenie usługi, takie jak oprogramowanie, sprzęt, dokumentacja, zostały zwrócone lub odzyskane w możliwej do wykorzystania formie, wraz ze wszelkimi danymi, programami, skryptami itp. posiadanymi przez organizację i przechowywanymi przez dostawcę usługi w chmurze. Jeżeli warunki usługi wymagają, aby dostawca chmury usunął dane, programy, kopie zapasowe oraz inne treści odbiorców chmury ze swojego środowiska, należy uzyskać i zweryfikować dowody, takie jak raporty lub logi systemowe, aby zapewnić, że informacje zostały prawidłowo usunięte [Len03].[29] Działania te powinny być prowadzone zgodnie z polityką zarządzania dokumentacją organizacji.

Posiadanie strategii wyjścia ustalonej we wczesnym etapie planowania, a także okresowe przeglądy i aktualizacje jej zawartości, mogą zminimalizować problemy związane z rozwiązaniem umowy o świadczenie usług oraz wysiłek wymagany do przeniesienia aplikacji do innego dostawcy usług lub przywrócenia ich do centrum danych organizacji.

5.5. PODSUMOWANIE ZALECEŃ

Tabela 4 poniżej podsumowuje zagadnienia i zalecenia, które mają zastosowanie na różnych etapach wykonywania usług podwykonawczych. Są one uzupełnieniem tych, które podano wcześniej w tabeli 2, a które wynikają z konkretnych kwestii związanych z bezpieczeństwem i ochroną prywatności.

[29] Więcej informacji na temat sanityzacji nośników można znaleźć w dokumencie NIST SP 800-88, Guidelines for Media Sanitization - http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88revl.pdf.

Tabela 4. Działania i rekomendacje dotyczące usług podwykonawstwa.

Obszary	Rekomendacje
Działania wstępne	Określenie wymogów bezpieczeństwa, ochrony prywatności i innych wymogów organizacyjnych, które muszą być spełnione przez usługi w chmurze, jako kryterium wyboru dostawcy chmury. Przeanalizowanie środków bezpieczeństwa i ochrony prywatności w środowisku dostawcy chmury oraz ocena poziomu ryzyka w odniesieniu do zakładanych przez organizację celów zabezpieczeń. Ocenienie zdolności i zobowiązania dostawcy chmury do świadczenia usług w chmurze w docelowych ramach czasowych oraz spełnienia określonych poziomów bezpieczeństwa i ochrony prywatności.
Działania inicjujące i współbieżne	Zapewnienie, że wszystkie wymogi umowne są wprost zapisane w umowie o świadczenie usług, w tym postanowienia dotyczące prywatności i bezpieczeństwa, oraz że są one zatwierdzone przez dostawcę usługi w chmurze. Zaangażowanie doradcy prawnego w przegląd umowy o świadczenie usług oraz we wszelkie negocjacje dotyczące warunków usługi. Ciągła ocena działania dostawcy usług chmurowych i jakości świadczonych usług w celu zapewnienia, że wszystkie zobowiązania wynikające z umowy są spełnione oraz w celu zarządzania i ograniczania ryzyka.
Działania podsumowujące	Powiadomienie dostawcy chmury o wszelkich wymogach umownych, które muszą być przestrzegane po rozwiązaniu umowy. Odwołanie wszystkich fizycznych i elektronicznych praw dostępu przypisanych dostawcy chmury oraz odzyskanie fizycznych tokenów i identyfikatorów w sposób terminowy. Zapewnienie, że zasoby organizacyjne udostępnione lub przechowywane przez dostawcę usługi w chmurze w ramach warunków umowy o świadczenie usług są zwracane lub odzyskiwane w użytecznej formie, a informacje zostały prawidłowo usunięte.

6. PODSUMOWANIE

Chmura obliczeniowa niesie ze sobą perspektywę daleko idących korzyści dla systemów i sieci organizacji. Nacisk na koszty i korzyści z wydajności publicznej chmury obliczeniowej powinien być zrównoważony z podstawowymi problemami bezpieczeństwa i ochrony prywatności, jakie organizacje mogą mieć z tymi środowiskami obliczeniowymi. Wiele z cech, które czynią chmurę obliczeniową atrakcyjną może być również sprzeczna z tradycyjnymi modelami i środkami bezpieczeństwa. Kilka krytycznych elementów technologii, takich jak rozwiązanie dla wspólnego zaufania, nie jest jeszcze w pełni zrealizowanych, co wpływa na skuteczne wdrożenia chmury obliczeniowej. Określenie bezpieczeństwa złożonych systemów komputerowych wspólnie skomponowanych jest również długotrwałym zagrożeniem bezpieczeństwa, które dotyka przetwarzanie na dużą skalę w ogóle, a chmury obliczeniowe w szczególności. Osiągnięcie wysokiego stopnia zaufania w implementacjach systemów było trudnym celem badaczy i praktyków bezpieczeństwa komputerowego i, jak pokazują przykłady podane w tym raporcie, jest to również zadanie do wykonania w przypadku przetwarzania w chmurze. Niemniej jednak, publiczna chmura obliczeniowa jest przekonującym paradygmatem obliczeniowym, który organizacje powinny rozważyć w swoim zbiorze rozwiązań informatycznych.

Odpowiedzialność za bezpieczeństwo i ochronę prywatności we wdrożeniach chmury publicznej nie może być delegowana do dostawcy chmury i jest obowiązkiem, który musi spełnić organizacja. Muszą one zapewnić, że każde wybrane rozwiązanie chmury publicznej jest skonfigurowane, wdrożone i zarządzane tak, aby spełniało wymogi bezpieczeństwa, ochrony prywatności i inne wymagania organizacji. Dane organizacji muszą być chronione w sposób zgodny z politykami, bez względu na to, czy znajdują się w centrum obliczeniowym organizacji, czy w chmurze. Organizacja musi zapewnić, że środki bezpieczeństwa i ochrony prywatności są zaimplementowane poprawnie i działają zgodnie z przeznaczeniem, przez cały cykl życia systemu.

Przejście do powierzania przetwarzania w chmurze publicznej jest na wiele sposobów ćwiczeniem w zarządzaniu ryzykiem. Zarządzanie ryzykiem wiąże się z identyfikacją i oceną ryzyka oraz podjęciem kroków w celu zredukowania go do akceptowalnego poziomu. Ocena i zarządzanie ryzykiem w systemach przetwarzania w chmurze wymaga ciągłego monitorowania stanu bezpieczeństwa systemu i może okazać się wyzwaniem, ponieważ znaczące części środowiska przetwarzania są pod kontrolą dostawcy chmury i prawdopodobnie poza zasięgiem organizacji. W całym cyklu życia systemu, zidentyfikowane ryzyka muszą być starannie zbilansowane z dostępnymi środkami bezpieczeństwa i ochrony prywatności oraz oczekiwanymi korzyściami z ich zastosowania. Zbyt duża liczba zabezpieczeń może być nieefektywna i nieskuteczna. Organizacje muszą zachować odpowiednią równowagę pomiędzy liczbą i siłą zabezpieczeń, a ryzykiem związanym z rozwiązaniami chmurowymi.

Chmura obliczeniowa to nowy paradygmat przetwarzania, który wciąż się rozwija. Oczekuje się, że postęp technologiczny poprawi wydajność i inne cechy usług oferowanych przez chmury publiczne, w tym prywatność i bezpieczeństwo. Wiele systemów organizacyjnych jest eksploatowanych przez długi czas i jeśli zostaną one przeniesione do chmury publicznej, prawdopodobnie doświadczą zmian technologicznych i innych w trakcie swojego funkcjonowania. Dostawcy chmur mogą zdecydować się na sprzedaż lub połączenie swoich ofert z innymi podmiotami; oferty usług mogą zostać wyparte przez oferty innego dostawcy chmury lub utracić popularność; ponadto organizacje mogą być zobowiązane do ponownego przeprowadzenia konkursu na istniejący kontrakt na usługi w chmurze, po upływie okresu obowiązywania umowy. Ostatecznie konieczność przeniesienia niektórych systemów do innej chmury publicznej jest realną ewentualnością, której organizacje nie mogą pominąć.

REFERENCJE

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA[30]	
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

[30] Narodowe Standardy Cyberbezpieczeństwa

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA[30]	
NSC 800-53	Zabezpieczenia i ochrona prywatności w systemach informacyjnych oraz organizacjach – na podstawie NIST SP 800-53
NSC 800-53A	Ocenianie środków bezpieczeństwa i ochrony prywatności w systemach informacyjnych oraz organizacjach. 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[31]	
[All88]	Julia Allen et al., Security for Information Technology Service Contracts, CMU/SEI-SIM-003, Software Engineering Institute, Carnegie Mellon University, January 1988, <URL: http://www.sei.cmu.edu/reports/98sim003.pdf>.
[Alp11]	Pavel Alpeyev, Joseph Galante, Mariko Yasu, Amazon.com Server Said to Have Been Used in Sony Attack, Bloomberg, May 14, 2011, <URL: http://www.bloomberg.com/news/2011-05-13/sony-network-said-to-have-been-invaded-by-hackers-using-amazon-com-server.html>.
[And11]	Nate Anderson, Anonymous vs. HBGary: the Aftermath, Ars Technica, February 24, 2011, <URL: http://arstechnica.com/tech-policy/news/2011/02/anonymous-vs-hbgary-the-aftermath.ars>.
[Arm10]	Michael Armbrust et al., A View of Cloud Computing, Communications of the ACM, Association for Computing Machinery, Vol. 53, No. 4, April 2010.
[Ash10]	Warwick Ashford, Google Confirms Dismissal of Engineer for Breaching Privacy Rules, Computer Weekly, September 16, 2010, <URL: http://www.computerweekly.com/Articles/2010/09/16/242877/Google-confirm-s-dismissal-of-engineer-for-breaching-privacy.htm>.

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

PUBLIKACJE ANGLOJĘZYCZNE[31]	
[Avo00]	Frederick M. Avolio, Best Practices in Network Security, Network Computing, March 20, 2000, <URL: http://www.networkcomputing.com/1105/1105f2.html>.
[Bar05]	Elaine B. Barker, William C. Barker, Annabelle Lee, Guideline for Implementing Cryptography In the Federal Government, NIST Special Publication 800-21, Second Edition, December 2005, <URL: http://csrc.nist.gov/publications/nistpubs/800-21-1/sp800-21-1_Dec2005.pdf>.
[Bin09]	David Binning, Top Five Cloud Computing Security Issues, Computer Weekly, April 24, 2009, <URL: http://www.computerweekly.com/Articles/2010/01/12/235782/Top-five-cloud-computing-security-issues.htm>.
[Bos11]	Bianca Bosker, Dropbox Bug Made Passwords Unnecessary, Left Data At Risk For Hours, The Huffington Post, June 21, 2011, <URL: http://www.huffingtonpost.com/2011/06/21/dropbox-security-bug-passwords_n_881085.html>.
[Bra10]	Simon Bradshaw, Christopher Millard, Ian Walden, Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services, Queen Mary School of Law Legal Studies, Research Paper No. 63/2010, September 2, 2010, <URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374>. 54
[Bra11]	Tony Bradley, Google, Skype, Yahoo Targeted by Rogue Comodo SSL Certificates, PCWorld, March 23, 2011, <URL: http://www.pcworld.com/businesscenter/article/223147/google_skype_yahoo_targeted_by_rogue_comodo_ssl_certificates.html>.

PUBLIKACJE ANGLOJĘZYCZNE[31]	
[Bro08]	Jon Brodkin, Loss of Customer Data Spurs Closure of Online Storage Service 'The Linkup,' Network World, August 11, 2008, <URL: http://www.networkworld.com/news/2008/081108-linkup-failure.html?page=1>.
[Bro09]	Carl Brooks, Amazon EC2 Attack Prompts Customer Support Changes, Tech Target, October 12, 2009, <URL: http://searchcloudcomputing.techtarget.com/news/article/0,289142,sid201_gci1371090,00.html>.
[Cal09]	Michael Calore, Ma.gnolia Suffers Major Data Loss, Site Taken Offline, Wired Magazine, January 30, 2009, <URL: http://www.wired.com/epicenter/2009/01/magnolia-suffer/>.
[CAO09]	Report from Office of the City Administrative Officer: Analysis of Proposed Contract, City of Los Angeles, CAO File No.:0150-00813-0001, July 9, 2009, <URL: http://clkrep.lacity.org/onlinedocs/2009/09-1714_rpt_cao_7-9-09.pdf>.
[Cap09]	Dawn Cappelli, Andrew Moore, Randall Trzeciak, Timothy J. Shimeall, Common Sense Guide to Prevention and Detection of Insider Threats, Third Edition, Version 3.1, CERT, January 2009, <URL: http://www.cert.org/archive/pdf/CSG-V3.pdf>.
[CBC04]	USA Patriot Act Comes under Fire in B.C. Report, CBC News, October 30, 2004, <URL: http://www.cbc.ca/canada/story/2004/10/29/patriotact_bc041029.html>.

PUBLIKACJE ANGLOJĘZYCZNE[31]	
[Cha10]	Rajarshi Chakraborty, Srilakshmi Ramireddy, T.S. Raghu, H. Raghav Rao, The Information Assurance Practices of Cloud Computing Vendors, IEEE IT Pro, Vol. 12, Issue 4, July/August 2010.
[Cho09]	Richard Chow et al., Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control, ACM Workshop on Cloud Computing Security, Chicago, Illinois, November 2009, <URL: http://www2.parc.com/csl/members/eshi/docs/ccsw.pdf>.
[CIO10a]	Privacy Recommendations for the Use of Cloud Computing by Federal Departments and Agencies, CIO Council, Privacy Committee, Web 2.0/Cloud Computing Subcommittee, August 2010, <URL: http://www.cio.gov/Documents/Privacy-Recommendations-Cloud-Computing-8-19-2010.docx>. 55
[CIO10b]	Federal Enterprise Architecture Security and Privacy Profile, Version 3, September 30, 2010, <URL: http://www.cio.gov/Documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf>.
[Cla09]	Gavin Clarke, Microsoft's Azure Cloud Suffers First Crash, The Register, March 16, 2009, <URL: http://www.theregister.co.uk/2009/03/16/azure_cloud_crash/>.
[CLA10]	Second Status Report on the Implementation of the Google E-Mail and Collaboration System, City Administrative Officer, City of Los Angeles, July 9, 2010, <URL: http://clkrep.lacity.org/onlinedocs/2009/09-1714_rpt_cao_7-9-10.pdf>.

PUBLIKACJE ANGLOJĘZYCZNE[31]

[CLA11a]	Second Amendment to Contract Number C-116359 between the City and Computer Sciences Corporation for E-Mail and Collaboration Solution (Google), Inter-Departmental Correspondence, City of Los Angeles, December 9, 2011, <URL: http://clkrep.lacity.org/onlinedocs/2009/09-1714-S2_RPT_CLA_12-09-11.pdf>.
[CLA11b]	Record of Council Action Regarding Second Amendment to Contract Number C-116359, City of Los Angeles, December 20, 2011, <URL: http://clkrep.lacity.org/onlinedocs/2009/09-1714-S2_CA_12-14-11.pdf>.
[Coc97]	Steve Cocheo, The Bank Robber, the Quote, and the Final Irony, nFront, American Bankers Association (ABA) Banking Journal, 1997, <URL: http://www.banking.com/aba/profile_0397.htm>.
[Cou09]	David A. Couillard, Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing, Minnesota Law Review, Vol. 93, No. 6, June 2009.
[Cra08]	George Craciun, Amazon EC2 Spreads Malware, Softpedia, July 1, 2008, <URL: http://news.softpedia.com/news/Amazon-EC2-Spreads-Malware-89014.shtml>.
[Cra10]	Personal conversation with Kevin K. Crawford, Assistant General Manager, Information Technology Agency, City of Los Angeles, December 15, 2010.
[Cra11]	Personal conversation with Kevin K. Crawford, Assistant General Manager, Information Technology Agency, City of Los Angeles, August 22, 2011.

PUBLIKACJE ANGLOJĘZYCZNE[31]	
[CSA11a]	Encryption and Key Management, Cloud Security Alliance, January 12, 2011, <URL: https://wiki.cloudsecurityalliance.org/guidance/index.php/Encryption_and_Key_Management>.
[CSA11b]	Cloud Controls Matrix, Version 1.2, Cloud Security Alliance, August 26, 2011, <URL: https://cloudsecurityalliance.org/wp-content/uploads/2011/08/CSA_CCM_v1.2.xls>. 56
[CSC10]	LA SECS Overview: SaaS E-mail and Collaboration Solution (SECS) – Implementing Google for the Los Angeles, CSC, April 15, 2010, <URL: http://assets1.csc.com/lef/downloads/LEFBriefing_CSC_LA_Google_041510.pdf>.
[CWD10]	Notice of Deficiencies-CSC Contract No. C-116359, City of Los Angeles, December 9, 2010, <URL: http://www.consumerwatchdog.org/resources/googdeficiency.pdf>.
[Daw05]	Alistair B. Dawson, Understanding Electronic Discovery and Solving Its Problems, 56th Annual Program on Oil and Gas Law, The Center for American and International Law, February 17-18, 2005, Houston, Texas, <URL: http://www.brsfirm.com/publications/docs/00037W.pdf>.
[Dem10]	Kelley Dempsey et al., Information Security Continuous Monitoring for Federal Information Systems and Organizations, Initial Public Draft, SP 800-137, NIST, September 2011, <URL: http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf>.

PUBLIKACJE ANGLOJĘZYCZNE[31]	
[Dig08]	Larry Dignam, Amazon Explains Its S3 Outage, ZDNET, February 16, 2008, <URL: http://www.zdnet.com/blog/btl/amazon-explains-its-s3-outage/8010>.
[Dij10]	Marten van Dijk, Ari Juels, On the Impossibility of Cryptography Alone for Privacy-Preserving Cloud Computing, 5th USENIX Workshop on Hot Topics in Security (HotSec '10), August 10, 2010, <URL: http://www.usenix.org/event/hotsec10/tech/full_papers/vanDijk.pdf>
[Din10]	Jocelyn Ding, LA's Move to Google Apps Continues Apace, Official Google Enterprise Blog, August 04, 2010, <URL: http://googleenterprise.blogspot.com/2010/08/las-move-to-google-apps-continues-apace.html>.
[DoC00]	Safe Harbor Privacy Principles, U.S. Department of Commerce, July 21, 2000, <URL: http://export.gov/safeharbor/eu/eg_main_018475.asp>.
[DPW10]	LA DPW Engineering Newsletter, No. 10-22, Los Angeles City, Department of Public Works (DPW), April 21, 2010, <URL: http://eng.lacity.org/newsletters/2010/04-21-10.pdf>.
[Dun10a]	John E. Dunn, Ultra-secure Firefox Offered to UK Bank Users, Techworld, February 26, 2010, <URL: http://news.techworld.com/security/3213740/ultra-secure-firefox-offered-to-uk-bank-users/>.

PUBLIKACJE ANGLOJĘZYCZNE[31]	
[Dun10b]	John E. Dunn, Virtualised USB Key Beats Keyloggers, Techworld, February 22, 2010, <URL: http://news.techworld.com/security/3213277/virtualised-usb-key-beats-keyloggers/>.
[DVA]	What the VA Is Doing to Protect Your Privacy, VA Pamphlet 005-06-1, Department of Veteran Affairs, <URL: http://www.privacy.va.gov/docs/VA005-06-1_privacy_brochure.pdf>.
[Eis05]	Margaret P. Eisenhauer, Privacy and Security Law Issues in Off-shore Outsourcing Transactions, Hunton & Williams LLP, The Outsourcing Institute, Legal Corner, February 15, 2005, <URL: http://www.outsourcing.com/legal_corner/pdf/Outsourcing_Privacy.pdf>.
[Fer07]	Peter Ferrie, Attacks on Virtual Machine Emulators, White Paper, Symantec Corporation, January 2007, <URL: http://www.symantec.com/avcenter/reference/Virtual_Machine_Threats.pdf>.
[Fer09]	Tim Ferguson, Salesforce.com Outage Hits Thousands of Businesses, CNET News, January 8, 2009, <URL: http://news.cnet.com/8301-1001_3-10136540-92.html>.
[Fer10]	David S. Ferreiro, Guidance on Managing Records in Cloud Computing Environments, NARA Bulletin 2010-05, September 8, 2010, <URL: http://www.archives.gov:80/records-mgmt/bulletins/2010/2010-05.html>.

PUBLIKACJE ANGLOJĘZYCZNE[31]	
[Fre08]	Stefan Frei, Thomas Duebendorfer, Gunter Ollmann, Martin May, Understanding the Web Browser Threat: Examination of vulnerable online Web browser populations and the "insecurity iceberg", ETH Zurich, Tech Report Nr. 288, 2008, <URL: http://e-collection.ethbib.ethz.ch/eserv/eth:30892/eth-30892-01.pdf>.
[Fow09]	Geoffrey Fowler, Ben Worthen, The Internet Industry Is on a Cloud – Whatever That May Mean, The Wall Street Journal, March 26, 2009, <URL: http://online.wsj.com/article/SB123802623665542725.html>.
[FTC07]	Fair Information Practice Principles, Federal Trade Commission, June 25, 2007, <URL: http://www.ftc.gov/reports/privacy3/fairinfo.shtm>.
[Gaj09]	Sebastian Gajek, Meiko Jensen, Lijun Liao, and Jörg Schwenk, Analysis of Signature Wrapping Attacks and Countermeasures, IEEE International Conference on Web Services, Los Angeles, California, July 2009.
[Gar05]	Tal Garfinkel, Mendel Rosenblum, When Virtual Is Harder than Real: Security Challenges in Virtual Machine Based Computing Environments, HotOS'05, Santa Fe, New Mexico, June 2005, <URL: http://www.stanford.edu/~talg/papers/HOTOS05/virtual-harder-hotos05.pdf>.
[Gar07]	Simson Garfinkel, An Evaluation of Amazon's Grid Computing Services: EC2, S3 and SQS, Technical Report TR-08-07, Center for Research on Computation and Society, School for Engineering and Applied Sciences, Harvard University, July 2007, <URL: http://simson.net/clips/academic/2007.Harvard.S3.pdf>.

PUBLIKACJE ANGLOJĘZYCZNE[31]	
[GAO06]	Privacy: Domestic and Offshore Outsourcing of Personal Information in Medicare, Medicaid, and TRICARE, United States Government Accountability Office, GAO-06-676, September 2006, <URL: http://www.gao.gov/new.items/d06676.pdf>.
[GAO10]	Contractor Integrity: Stronger Safeguards Needed for Contractor Access to Sensitive Information, United States Government Accountability Office, GAO-10-693, September 2010, <URL: http://www.gao.gov/new.items/d10693.pdf>.
[Gee08]	Daniel E. Geer, Complexity Is the Enemy, IEEE Security and Privacy, Vol. 6, No. 6, November/December 2008.
[Gon09]	Reyes Gonzalez, Jose Gasco, and Juan Llopis, Information Systems Outsourcing Reasons and Risks: An Empirical Study, International Journal of Human and Social Sciences, Vol. 4, No. 3, 2009, <URL: http://www.waset.org/journals/ijhss/v4/v4-3-24.pdf>.
[Goo09a]	Dan Goodin, Salesforce.com Outage Exposes Cloud's Dark Linings, The Register, January 6, 2009, <URL: http://www.theregister.co.uk/2009/01/06/salesforce_outage/>.
[Goo09b]	Dan Goodin, Webhost Hack Wipes Out Data for 100,000 Sites, The Register, June 8, 2009, <URL: http://www.theregister.co.uk/2009/06/08/webhost_attack/>.
[Goo10]	Dan Goodin, Privacy Watchdog Pack Demands Facebook Close the 'App Gap', The Register, June 16, 2010, <URL: http://www.theregister.co.uk/2010/06/16/facebook_privacy/>.

PUBLIKACJE ANGLOJĘZYCZNE[31]	
[Gou11]	Jeff Gould, Los Angeles Ends Google Apps for LAPD; Decision Bigger Than You Think, AOL Government, December 19, 2011, <URL: http://gov.aol.com/2011/12/19/los-angeles-ends-google-apps-for-lapd-decision-bigger-than-you/>.
[Gra03]	Tim Grance et al., Guide to Information Technology Security Services, Special Publication 800-35, National Institute of Standards and Technology, October 2003, <URL: http://csrc.nist.gov/publications/nistpubs/800-35/NIST-SP800-35.pdf>.
[Gre09]	Andy Greenberg, IBM's Blindfolded Calculator, Forbes Magazine, July 13, 2009, <URL: http://www.forbes.com/forbes/2009/0713/breakthroughs-privacy-super-secret-encryption.html>.
[Gro10]	Bernd Grobauer, Thomas Schreck, Towards Incident Handling in the Cloud: Challenges and Approaches, ACM Cloud Computing Security Workshop, Chicago, Illinois, October 8, 2010.
[Gru09]	Nils Gruschka, Luigi Lo Iacono, Vulnerable Cloud: SOAP Message Security Validation Revisited, IEEE International Conference on Web Services, Los Angeles, California, July 2009.
[Gun08]	Mike Gunderloy, Who Protects Your Cloud Data?, Web Worker Daily, January 13, 2008, <URL: http://webworkerdaily.com/2008/01/13/who-protects-your-cloud-data/>.

PUBLIKACJE ANGLOJĘZYCZNE[31]	
[Han06]	Saul Hansell, Online Trail Can Lead To Court, The New York Times, February 4, 2006, <URL: http://query.nytimes.com/gst/fullpage.html?res=9B03E5D7163EF937A35751C0A9609C8B63>.
[HR2458]	Federal Information Security Management Act of 2002 (FISMA), H.R. 2458, Title III—Information Security, <URL: http://csrc.nist.gov/drivers/documents/FISMA-final.pdf>.
[Inf09]	Twitter Email Account Hack Highlights Cloud Dangers, Infosecurity Magazine, July 23, 2009, <URL: http://www.infosecurity-magazine.com/view/2668/twitter-email-account-hack-highlights-cloud-dangers-/>.
[Jac07]	Dean Jacobs, Stefan Aulbach, Ruminations on Multi-Tenant Databases, Fachtagung für Datenbanksysteme in Business, Technologie und Web, Aachen, Germany, March 5-9, 2007, <URL: http://www.btw2007.de/paper/p514.pdf>.
[Jan08]	Wayne Jansen, Karen Scarfone, Guidelines on Cell Phone and PDA Security, Special Publication (SP) 800-124, National Institute of Standards and Technology, October 2008, <URL: http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf>
[Jen09]	Meiko Jensen, Jörg Schwenk, Nils Gruschka, Luigi Lo Iacono, On Technical Security Issues in Cloud Computing, IEEE International Conference on Cloud Computing, Bangalore, India, September 21-25, 2009.

PUBLIKACJE ANGLOJĘZYCZNE[31]	
[JTF10]	Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, Joint Task Force Transformation Initiative, NIST Special Publication 800-37, Revision 1, <URL: http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>.
[Kan09]	Balachandra Reddy Kandukuri, Ramakrishna Paturi V, Atanu Rakshit, Cloud Security Issues, IEEE International Conference on Services Computing, Bangalore, India, September 21-25, 2009.
[Kar08]	Paul A. Karger, I/O for Virtual Machine Monitors: Security and Performance Issues, IEEE Security and Privacy, September/October 2008.
[Kat10]	Neil Katz, Austin Plane Crash: Pilot Joseph Andrew Stack May Have Targeted IRS Offices, Says FBI, CBS News, February 18, 2010, <URL: http://www.cbsnews.com/8301-504083_162-6220271-504083.html?tag=contentMain%3bcontentBody>.
[Kel05]	Yared Keleta, J.H.P. Eloff, H.S. Venter, Proposing a Secure XACML Architecture Ensuring Privacy and Trust, Research in Progress Paper, University of Pretoria, 2005, <URL: http://icsa.cs.up.ac.za/issa/2005/Proceedings/Research/093_Article.pdf>.
[Ker10]	Sean Michael Kerner, Mozilla Confirms Security Threat from Malicious Firefox Add-ons, eSecurity Planet, February 5, 2010, <URL: http://www.esecurityplanet.com/news/article.php/3863331/Mozilla-Confirms-Security-Threat-From-Malicious-Firefox-Add-Ons.htm>.

PUBLIKACJE ANGLOJĘZYCZNE[31]

[Ker11]	Justin Kern, Amazon Apologizes, Cites Human Error in Cloud Interruption, Information Management Online, April 29, 2011, <URL: http://www.information-management.com/news/cloud_SaaS_data_center_downtime_storage_Amazon-10020215-1.html>.
[Kin06]	Samuel King, Peter Chen, Yi-Min Wang, Chad Verbowski, Helen Wang, Jacob Lorch, SubVirt: Implementing Malware with Virtual Machines, IEEE Symposium on Security and Privacy, Berkeley, California, May 2006, <URL: http://www.eecs.umich.edu/~pmchen/papers/king06.pdf>.
[Kre07]	Brian Krebs, Salesforce.com Acknowledges Data Loss, Security Fix, The Washington Post, November 6, 2007, <URL: http://blog.washingtonpost.com/securityfix/2007/11/salesforcecom_acknowledges_dat.html>.
[Kre08]	Brian Krebs, Amazon: Hey Spammers, Get Off My Cloud! The Washington Post, July 1, 2008, <URL: http://voices.washingtonpost.com/securityfix/2008/07/amazon_hey_spammers_get_off_my.html>.
[Kow08]	Eileen Kowalski et al., Insider Threat Study: Illicit Cyber Activity in the Government Sector, U.S. Secret Service and Carnegie Mellon University, Software Engineering Institute, January 2008, <URL: http://www.cert.org/archive/pdf/insiderthreat_gov2008.pdf>.
[Kri08]	Michael Krigsma, Amazon S3 Web Services Down. Bad, Bad News for Customers, ZDNET, February 15, 2008, <URL: http://blogs.zdnet.com/projectfailures/?p=602>.

PUBLIKACJE ANGLOJĘZYCZNE[31]	
[Kum08]	Sushil Kumar, Oracle Database Backup in the Cloud, White Paper, Oracle Corporation, September 2008.
[Lab95]	Stephen Labaton, 2 Men Held in Attempt to Bomb I.R.S. Office, New York Times, December 29, 1995, <URL: http://www.nytimes.com/1995/12/29/us/2-men-held-in-attempt-to-bomb-irs-office.html?pagewanted=1>.
[LAPD10]	Supplemental Report to the City Administrative Officer: Second Status Report on the Implementation of the Google E-Mail and Collaboration System (C.F. 09-1714), Los Angeles Police Department, City of Los Angeles, <URL: http://clkrep.lacity.org/onlinedocs/2009/09-1714_rpt_lapd_7-8-10.pdf>.
[Lat96]	20-Year Term in Plot to Bomb IRS Offices, Nation In Brief, Los Angeles Times, August 10, 1996, <URL: http://articles.latimes.com/1996-08-10/news/mn-32970_1_20-year-term>.
[Lea09]	Neal Leavitt, Is Cloud Computing Really Ready for Prime Time?, IEEE Computer, January 2009.
[Len03]	Bee Leng, A Security Guide for Acquiring Outsourced Service, GIAC GSEC Practical (v1.4b), SANS Institute, August 19, 2003, <URL: http://www.sans.org/reading_room/whitepapers/services/a_security_guide_for_acquiring_outsourced_service_1241>.

PUBLIKACJE ANGLOJĘZYCZNE[31]	
[Mag10]	James Maguire, How Cloud Computing Security Resembles the Financial Meltdown, Datamation, internet.com, April 27, 2010, <URL: http://itmanagement.earthweb.com/netsys/article.php/3878811/How-Cloud-Computing-Security-Resembles-the-Financial-Meltdown.htm>.
[Mcc10]	Erika McCallister, Tim Grance, Karen Scarfone, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), SP 800-122, National Institute of Standards and Technology, April 2010, <URL: http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>.
[Mcd10]	Steve McDonald, Legal and Quasi-Legal Issues in Cloud Computing Contracts, Workshop Document, EDUCAUSE and NACUBO Workshop on Cloud Computing and Shared Services, Tempe, Arizona, February 8–10, 2010, <URL: http://net.educause.edu/section_params/conf/CCW10/issues.pdf> .
[Mcm07]	Robert McMillan, Salesforce.com Warns Customers of Phishing Scam, PC Magazine, IDG News Network, November 6, 2007, <URL: http://www.pcworld.com/businesscenter/article/139353/salesforcecom_warns_customers_of_phishing_scam.html>.
[Mcm09a]	Robert McMillan, Hackers Find a Home in Amazon's EC2 Cloud, Infoworld, IDG News Network, December 10, 2009, <URL: http://www.infoworld.com/d/cloud-computing/hackers-find-home-in-amazons-ec2-cloud-742>.

PUBLIKACJE ANGLOJĘZYCZNE[31]	
[Mcm09b]	Robert McMillan, Misdirected Spyware Infects Ohio Hospital, PC Magazine, IDG News Service September 17, 2009, <URL: http://www.pcworld.com/businesscenter/article/172185/misdirected_spyware_infects_ohio_hospital.html>.
[Mee09]	Haroon Meer, Nick Arvanitis, Marco Slaviero, Clobbering the Cloud, Part 4 of 5, Black Hat USA Talk Write-up, SensePost SDH Labs, 2009, <URL: http://www.sensepost.com/labs/conferences/clobbering_the_cloud/amazon>.
[Mel11]	Peter Mell, Tim Grance, The NIST Definition of Cloud Computing, Special Publication 800-145, National Institute of Standards and Technology, August 2011, <URL: http://csrc.nist.gov/publications/nistpubs/800-145/sp800-145.pdf>.
[Met09]	Cade Metz, DDoS Attack Rains Down on Amazon Cloud, The Register, October 5, 2009, <URL: http://www.theregister.co.uk/2009/10/05/amazon_bitbucket_outage/>.
[Met11]	Cade Metz, Amazon Cloud Fell from Sky after Botched Network Upgrade, The Register, April 29, 2011, <URL: http://www.theregister.co.uk/2011/04/29/amazon_ec2_outage_post_mortem/>.
[Mic09]	The Windows Azure Malfunction This Weekend, Windows Azure <Team Blog>, Microsoft Corporation, March 18, 2009, <URL: http://blogs.msdn.com/windowsazure/archive/2009/03/18/the-windows-azure-malfunction-this-weekend.aspx>.

PUBLIKACJE ANGLOJĘZYCZNE[31]	
[Mic10]	Fact-Based Comparison of Hosted Services: Google vs. Microsoft, Microsoft Corporation, May 16, 2010, <URL: http://download.microsoft.com/download/0/5/F/05FF69ED-6F8F-4357-863B-12E27D6F1115/Hosted%20Services%20Comparison%20Whitepaper%20-%20Google%20vs%20Microsoft.pdf>.
[Mil08]	Rich Miller, Major Outage for Amazon S3 and EC2, Data Center Knowledge, February 15, 2008, <URL: http://www.datacenterknowledge.com/archives/2008/02/15/major-outage-for-amazon-s3-and-ec2/>.
[Mil09]	Rich Miller, Lightning Strike Triggers Amazon EC2 Outage, Data Center Knowledge, June 11, 2009, <URL: http://www.datacenterknowledge.com/archives/2009/06/11/lightning-strike-triggers-amazon-ec2-outage/>.
[Mod08]	Austin Modine, Downed Salesforce Systems Slow Europe and US, The Register, February 11, 2008, <URL: http://www.theregister.co.uk/2008/02/11/salesforce_outages_feb_2008/>.
[MRG10]	Online Banking: Browser Security Project, Malware Research Group, Zorin Nexus Ltd., June 2010, <URL: http://malwareresearchgroup.com/wp-content/uploads/2009/01/Online-Banking-Browser-Security-Project-June-201013.zip>.
[Mul10]	Robert Mullins, The Biggest Cloud on the Planet is Owned by the Crooks, Network World, March 22, 2010, <URL: http://www.networkworld.com/community/node/58829>.

PUBLIKACJE ANGLOJĘZYCZNE[31]	
[Nav10]	Eliminating the Data Security and Regulatory Concerns of Using SaaS Applications, White Paper, Navajo Systems, January 2010, <URL: http://www.navajosystems.com/media/Virtual_Private_SaaS_White_Paper.pdf>.
[Obe08a]	Jon Oberheide, Evan Cooke, Farnam Jahanian, Empirical Exploitation of Live Virtual Machine Migration, Black Hat Security Conference, Washington, DC, February 2008, <URL: http://www.blackhat.com/presentations/bh-dc-08/Oberheide/Whitepaper/bh-dc-08-oberheide-WP.pdf>.
[Obe08b]	Jon Oberheide, Evan Cooke, Farnam Jahanian, CloudAV: N-Version Antivirus in the Network Cloud, USENIX Security Symposium, Association, San Jose, CA, July 28-August 1, 2008, <URL: http://www.eecs.umich.edu/fjgroup/pubs/usenix08-cloudav.pdf>.
[OECD80]	OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Organisation for Economic Co-operation and Development, September 23,1980, <URL: http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00.html>.
[Opp03]	David Oppenheimer, Archana Ganapathi, David Patterson, Why Do Internet Services Fail, and What Can Be Done About It?, 4th USENIX Symposium on Internet Technologies and Systems, March 2003, <URL: http://roc.cs.berkeley.edu/papers/usits03.pdf>.

PUBLIKACJE ANGLOJĘZYCZNE[31]	
[Orm07]	Tavis Ormandy, An Empirical Study into the Security Exposure to Hosts of Hostile Virtualized Environments, 2007, <URL: http://taviso.decsystem.org/virtsec.pdf>.
[Ove10]	Stephanie Overby, How to Negotiate a Better Cloud Computing Contract, CIO, April 21, 2010, <URL: http://www.cio.com/article/591629/How_to_Negotiate_a_Better_Cloud_Computing_Contract>.
[Owa10]	Cloud-10 Multi Tenancy and Physical Security, The Open Web Application Security Project, Cloud Top 10 Security Risks, August 30, 2010, <URL: https://www.owasp.org/index.php/Cloud-10_Multi_Tenancy_and_Physical_Security>.
[Pea09]	Siani Pearson, Taking Account of Privacy When Designing Cloud Computing Services, International Conference on Software Engineering (ICSE) Workshop on Software Engineering Challenges of Cloud Computing, Vancouver, Canada, May 23, 2009.
[Pep11a]	Julianne Pepitone, Amazon EC2 Outage Downs Reddit, Quora, CNN Money, April 22, 2011, <URL: http://money.cnn.com/2011/04/21/technology/amazon_server_outage/index.htm>.
[Pep11b]	Julianne Pepitone, RSA Offers to Replace All SecurID Tokens after Hack Attack, CNN Money Tech, June 8, 2011, <URL: http://money.cnn.com/2011/06/08/technology/securid_hack/index.htm>.

PUBLIKACJE ANGLOJĘZYCZNE[31]

[Per11]	By Juan Carlos Perez, Microsoft's Cloud BPOS Suite Suffers Outage Again, InfoWorld Inc., June 22, 2011, <URL: http://www.infoworld.com/d/applications/microsofts-cloud-bpos-suite-suffers-outage-again-050>.
[Pon10]	Larry Ponemon, Security of Cloud Computing Users, Ponemon Institute, May 12, 2010, <URL: http://www.ca.com/files/IndustryResearch/security-cloud-computing-users_235659.pdf>.
[Pro07]	Niels Provos, Dean McNamee, Panayiotis Mavrommatis, Ke Wang, Nagendra Modadugu, The Ghost in the Browser: Analysis of Web-based Malware, Hot Topics in Understanding Botnets (HotBots), April 10, 2007, Cambridge, Massachusetts, <URL: http://www.usenix.org/events/hotbots07/tech/full_papers/provos/provos.pdf>.
[Pro09]	Niels Provos, Moheeb Abu Rajab, Panayiotis Mavrommatis, Cybercrime 2.0: When the Cloud Turns Dark, Communications of the ACM, April 2009.
[Pro10]	Cloud Security and Privacy: Data Security and Storage, November 18, 2010, <URL http://mscerts.programming4.us/programming/Cloud%20Security%20and%20Privacy%20%20%20Data%20Security%20and%20Storage.aspx>.
[Rag09]	Steve Ragan, New Service Offers Cloud Cracking for WPA, The Tech Herald, December 8, 2009, <URL: http://www.thetechherald.com/article.php/200950/4906/New-service-offers-cloud-cracking-for-WPA>.

PUBLIKACJE ANGLOJĘZYCZNE[31]

[Rap09]	J.R. Raphael, Facebook Privacy Change Sparks Federal Complaint, PC World, February 17, 2009, <URL: http://www.pcworld.com/article/159703/facebook.html?tk=rel_news>.
[Ref10]	Security Within a Virtualized Environment: A New Layer in Layered Security, White Paper, Reflex Security, retrieved April 23, 2010, <URL: http://www.vmware.com/files/pdf/partners/security/security-virtualized-whitepaper.pdf>.
[Ris09]	Thomas Ristenpart, Eran Tromer, Hovav Shacham, Stefan Savage, Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds, ACM Conference on Computer and Communications Security, November 2009, <URL: http://cseweb.ucsd.edu/~hovav/dist/cloudsec.pdf>.
[Row07]	Brent R. Rowe, Will Outsourcing IT Security Lead to a Higher Social Level of Security?, Research Triangle Institute International, July 2007, <URL: http://weis2007.econinfosec.org/papers/47.pdf>.
[Sar10]	David Sarno, Los Angeles Police Department Switch to Google E-mail System Hits Federal Roadblock, Los Angeles Times, November 03, 2010, <URL: http://articles.latimes.com/2010/nov/03/business/la-fi-google-la-20101103>.
[Sar11a]	David Sarno, Google Facing Hurdles in Bid to Provide Email Service to Governments, Los Angeles Times, April 14, 2011, <URL: http://articles.latimes.com/2011/apr/14/business/la-fi-google-email-20110414>.

PUBLIKACJE ANGLOJĘZYCZNE[31]	
[Sar11b]	David Sarno, L.A. won't put LAPD on Google's cloud-based email system, Los Angeles Times, December 14, 2011, <URL: http://articles.latimes.com/2011/dec/14/business/la-fi-google-email-20111215>.
[Sca11]	Karen Scarfone, Murugiah Souppaya, Paul Hoffman, Guide to Security for Full Virtualization Technologies, Special Publication 800-125, National Institute of Standards and Technology, January 2011, <URL: http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf >.
[Sch00]	Bruce Schneier, Crypto-Gram Newsletter, Software Complexity and Security, March 15, 2000, <URL: http://www.schneier.com/crypto-gram-0003.html#8>.
[Sch10]	Jeff Schnepper, Don't Like the Tax Law? Don't Shoot the IRS, MSN, March 10, 2010, <URL: http://articles.moneycentral.msn.com/Taxes/blog/page.aspx?post=1692029&_blg=1,1619827>.
[Sch11]	Mathew J. Schwartz, Are You Ready for an FBI Server Takedown?, Information Week, July 01, 2011, <URL: http://www.informationweek.com/news/security/management/231000897>.
[Sha08]	Amit Shah, Kernel-based Virtualization with KVM, Linux Magazine, issue 86, January 2008, <URL: http://www.linux-magazine.com/w3/issue/86/Kernel_Based_Virtualization_With_KVM.pdf>.

PUBLIKACJE ANGLOJĘZYCZNE[31]	
[Sec05]	VMware Vulnerability in NAT Networking, BugTraq, SecurityFocus, December 21, 2005, <URL: http://www.securityfocus.com/archive/1/420017 and http://www.securityfocus.com/bid/15998/>.
[SECS09]	Professional Services Contract, SAAS E-Mail & Collaboration Solution (SECS), City of Los Angeles, November 10, 2009, <URL: https://sites.google.com/a/lageecs.lacity.org/la-geecs-blog/home/faqs-1/C-116359_c_11-20-09.pdf?attredirects=0&d=1>
[She05]	Tim Shelton, Remote Heap Overflow, ACSSEC-2005-11-25 - 0x1, <URL: http://packetstormsecurity.org/0512-advisories/ACSSEC-2005-11-25-0x1.txt>.
[Sla09]	Marco Slaviero, BlackHat Presentation Demo Vids: Amazon, part 4 of 5, AMIBomb, August 8, 2009, <URL: http://www.sensepost.com/blog/3797.html>.
[Sob06]	Charles H. Sobey, Laslo Orto, and Glenn Sakaguchi, Drive-Independent Data-Recovery: The Current State-of-the-Art, IEEE Transactions on Magnetics, February 2006, <URL: http://www.actionfront.com/whitepaper/Drive%20Independent%20Data%20Recovery%20TMRC2005%20Preprint.pdf>.
[Som11]	Juraj Somorovsky et al., All Your Clouds Belong to Us – Security Analysis of Cloud Management Interfaces, ACM Cloud Computing Security Workshop (CCSW), Chicago, October 21, 2011.

PUBLIKACJE ANGLOJĘZYCZNE[31]	
[Sto02]	Gary Stoneburner, Alice Goguen, and Alexis Feringa, Risk Management Guide for Information Technology Systems, SP 800-30, NIST, July 2002, <URL: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>.
[Sto10]	Jon Stokes, EMC's Atmos Shutdown Shows Why Cloud Lock-in is Still Scary, Ars Technica, July 2010, <URL: http://arstechnica.com/business/news/2010/07/emcs-atmos-shutdown-shows-why-cloud-lock-in-is-still-scary.ars>.
[Sut09]	John D. Sutter, Twitter Hack Raises Questions about 'Cloud Computing', CNN, July 16, 2009, <URL: http://edition.cnn.com/2009/TECH/07/16/twitter.hack/>.
[Swa06]	Marianne Swanson, Joan Hash, Pauline Bowen, Guide for Developing Security Plans for Federal Information Systems, NIST, Special Publication 800-18, Revision 1, February 2006, <URL: http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf>.
[UCG10]	Cloud Computing Use Cases White Paper, Version 4.0, Cloud Computing Use Case Discussion Group, July 2, 2010, <URL: http://opencloudmanifesto.org/Cloud_Computing_Use_Cases_Whitepaper-4_0.pdf>.

PUBLIKACJE ANGLOJĘZYCZNE[31]	
[Val08]	Craig Valli, Andrew Woodward, The 2008 Australian Study of Remnant Data Contained on 2nd Hand Hard Disks: The Saga Continues, The 6th Australian Digital Forensics Conference, Perth, Western Australia, December 1-3, 2008, <URL: http://conferences.secau.org/proceedings/2008/forensics/Valli%20and%20Woodward%202008%20remnant%20Data%20saga%20continues.pdf>.
[Vaq09]	Luis M. Vaquero1, Luis Rodero-Merino1, Juan Caceres, Maik Lindner, A Break in the Clouds: Towards a Cloud Definition, Computer Communication Review (CCR) Online, Short technical Notes, January 2009, <URL: http://ccr.sigcomm.org/online/files/p50-v39n1l-vaqueroA.pdf>.
[Vie09]	Kleber Vieira, Alexandre Schulter, Carlos Westphall, Carla Westphall, Intrusion Detection Techniques in Grid and Cloud Computing Environment, IT Professional, IEEE Computer Society, August 26, 2009.
[Vij11]	Jaikumar Vijayan, City of Los Angeles May Sue over Delays in Google Apps Project, Computer World, April 18, 2011, <URL: http://computerworld.co.nz/news.nsf/management/city-of-los-angeles-may-sue-over-delays-in-google-apps-project-report>.
[Vmw09]	VMware Hosted Products and Patches for ESX and ESXi Resolve a Critical Security Vulnerability, VMware Security Advisory, VMSA-2009-0006, <URL: http://www.vmware.com/security/advisories/VMSA-2009-0006.html>.

PUBLIKACJE ANGLOJĘZYCZNE[31]	
[Vmw10]	VMware vShield: Virtualization-Aware Security for the Cloud, product brochure, 2010, <URL: http://www.vmware.com/files/pdf/vmware-vshield_br-en.pdf>.
[Wai08]	Phil Wainewright. Many Degrees of Multi-tenancy, ZDNET News and Blogs, June 16, 2008, <URL: http://blogs.zdnet.com/SAAS/?p=533>.
[Wal10]	Hannah Wald, Cloud Computing for the Federal Community, IAnewsletter, Vol. 13, No. 2, Information Assurance Technology Analysis Center, Spring 2010.
[Wei09]	Jinpeng Wei, Xiaolan Zhang, Glenn Ammons, Vasanth Bala, Peng Ning, Managing Security of Virtual Machine Images in a Cloud Environment, ACM Cloud Computing Security Workshop (CCSW'09) , Chicago, Illinois, November 13, 2009.
[Wei11]	Thilo Weichert, Cloud Computing and Data Privacy, The Sedona Conference, Working Group on International Electronic Information Management, Discovery & Disclosure, February 2011, <URL: https://www.datenschutzzentrum.de/cloud-computing/20100617-cloud-computing-and-data-privacy.pdf>.
[Whi09]	Lance Whitney, Amazon EC2 Cloud Service Hit by Botnet, Outage, December 11, 2009, CNET News, <URL: http://news.cnet.com/8301-1009_3-10413951-83.html>.
[Wil10]	Matt Williams, All Eyes are on Los Angeles as City Deploys Cloud-Based E-Mail, Government Technology, February 10, 2010, <URL: http://www.govtech.com/gt/744804?id=744804&full=1&story_pg=1>.

PUBLIKACJE ANGLOJĘZYCZNE[31]	
[Xen08]	Xen Architecture Overview, Version 1.2, Xen Wiki Whitepaper, February 13, 2008, <URL: http://wiki.xensource.com/xenwiki/XenArchitecture?action=AttachFile&do=get&target=Xen+Architecture_Q1+2008.pdf>.
[You07]	Greg Young, Neil MacDonald, John Pescatore, Limited Choices are Available for Network Firewalls in Virtualized Servers, Gartner, Inc., ID Number: G00154065, December 20, 2007, <URL: http://www.reflexsystems.com/Content/News/20071220-GartnerVirtualSecurityReport.pdf>.
[You08]	Lamia Youseff, Maria Butrico, Dilma Da Silva, Toward a Unified Ontology of Cloud Computing, Grid Computing Environments Workshop (GCE08), held in conjunction with SC08, November 2008, <URL: http://www.cs.ucsb.edu/~lyouseff/CCOntology/CloudOntology.pdf>.
[Zet09a]	Kim Zetter, FBI Defends Disruptive Raids on Texas Data Centers, Wired Magazine, April 7, 2009, <URL: http://www.wired.com/threatlevel/2009/04/data-centers-ra/>.
[Zet09b]	Kim Zetter, Bank Sends Sensitive E-mail to Wrong Gmail Address, Sues Google, Wired Magazine, September 21, 2009, <URL: http://www.wired.com/threatlevel/2009/09/bank-sues-google/>.

ZAŁĄCZNIK A SŁOWNIK I AKRONIMY

PATRZ: NSC 7298, *SŁOWNIK KLUCZOWYCH POJĘĆ Z ZAKRESU CYBERBEZPIECZEŃSTWA*

ZAŁĄCZNIK B ZASOBY INTERNETOWE

Poniższa tabela zawiera listę dostępnych materiałów internetowych, które mogą być pomocne dla specjalistów ds. bezpieczeństwa oraz innych czytelników niniejszej publikacji w uzyskaniu lepszego zrozumienia kwestii bezpieczeństwa i ochrony prywatności w chmurze obliczeniowej oraz możliwych środków zaradczych.

Opis zasobu	URL
DRAFT Cloud Computing Synopsis and Recommendations, NIST, May 2011	http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf
Challenging Security Requirements for US Government Cloud Computing Adoption (Draft), Cloud Security Working Group, NIST, November 2011	http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/CloudSecurity/NIST_Security_Requirements_for_US_Government_Cloud.pdf
Top Threats to Cloud Computing, V1.0, Cloud Security Alliance, March 2010	http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf
Privacy Recommendations for the Use of Cloud Computing by Federal Departments and Agencies, CIO Council, Privacy Committee, August 19,2010	http://www.cio.gov/documents/Privacy-Recommendations-Cloud-Computing-8-19-2010.docx
Security Guidance For Critical Areas of Focus in Cloud Computing, V2.1, Cloud Security Alliance, December 2009	http://www.cloudsecurityalliance.org/csaguide.pdf

Opis zasobu	URL
Cloud Computing Risk Assessment, European Network and Information Security Agency, November 2009	http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport
The 10 Worst Cloud Outages (and what we can learn from them), J R Raphael, InfoWorld, June 27, 2011	http://www.infoworld.com/d/cloud-computing/the-10-worst-cloud-outages-and-what-we-can-learn-them-902
The Future of Cloud Computing, Version 1.0, Commission of the European Communities, Expert Group on Cloud Computing, January 2010	http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf