Raport nr 8
Niniejszy raport został napisany na podstawie dokumentów Departamentu Stanu USA ze zbioru „The Threads In Cybersecurity" a także Cloud Security Alliance "Security Guidance for Critical Areas in Cloud Computing" oraz w "Top Threats to Cloud Computing".

1. Wstęp

W przypadku Cloud Computing istnieją znaczące ryzyka zarówno dotyczące samych usług jak i finansowej stabilności ich operatora. Przez swoją naturę zakładającą swobodną wymianę danych Cloud Computing zawiera w sobie także , szereg ryzyk dla klienta. Główne zagrożenia sformułowane w dokumentach Departamentu Stanu i Cloud Security Alliance są następujące:

- Nadużycie i użycie w celu przestępczym Cloud Computing
- Niebezpieczne API
- Wrogie działania wewnątrz Chmury
- Luki w aplikacjach i mechanizmach Shared Technology
- Wycieki lub utrata danych
- Przechwycenie usługi, ruchu lub konta
- Ryzyko nieznanego poziomu

Dokumenty CSA oraz Departamentu Stanu nie podzieliły tych zagrożeń według istotności, nie przydzieliły im też określonych wag. Nawet bowiem skumulowane rankingi nie przyniosły dostatecznej ilości danych dla określenia, które z nich należy uznać za najistotniejsze i stworzenia na ich podstawie uniwersalnego profilu zagrożeń.
Nie dla wszystkich przy tym rekomendacje dotyczące wagi i sposobów likwidacji zagrożeń będą istotne. Część firm bowiem przechowuje w chmurze tylko dane o niskiej wrażliwości, należące do klientów podczas gdy w przypadku innych usługodawców są przechowywane także krytyczne dane klientów. Niektóre aplikacje chmury przechowują dane personalne, do których dostęp jest regulowany prawnie i na tym opiera się głównie fundament ich obrony przed niepowołanym dostępem. Inne posiadają oparty na rozwiązaniach chmury zewnętrzny system obrony przez zagrożeniami. Wobec tego zróżnicowania jest konieczne dla klienta chmury, aby określił jakie wartości organizacji można przenieść do takiego systemu. Ponadto rekomendacje CSA i innych instytucji, dotyczące zagrożeń, muszą być wprowadzane przy użyciu najlepszych znanych praktyk biznesowych i przy stałej znajomości kontekstu misji biznesowej, ryzyk, zwrotów oraz zagrożeń w środowisku chmury.
Jeśli chodzi o pomiar ryzyk, stosunkowo najniższym wydaje się Ryzyko Nieznanego Poziomu, chociaż komentarze analityków precyzują, że po prostu należy ściśle określić co kryje się za tym terminem. Niewykluczone więc, że zostanie on dopracowany w następnych edycjach raportów CSA i innych organizacji, a zwłaszcza Departamentu Stanu i Departamentu Obrony dla agend rządowych i administracji.
Pozostałe ryzyka mają w rzeczywistości wagę uzależnioną od biznesu prowadzonego przez przedsiębiorstwo. I tak Niebezpieczne API stanowią istotne zagrożenie w przypadku projektu zakładającego wypuszczanie na rynek aplikacji line-of-business projektowanych przy użyciu PaaS (Platform As Service), co podpowiada uważną obserwację bezpieczeństwa aplikacji przy zastosowaniu praktyk jej tworzenia i zabezpieczania jak SDLC (software development lifecycle). W przypadku luki w mechanizmach Shared Technology, zagrożenie to jest najistotniejsze dla firm używających masowo wirtualizacji.

Definicje:
Saas (Software As Service) – podstawowy model Cloud Computing, gdzie aplikacja jest przechowywana w Internecie i udostępniania w ramach usług w chmurze.

PaaS (Platform As Service) – model w którym udostępniane jest wirtualne środowisko pracy. Zwykle dotyczy to firm ITC lub firm o skomplikowanym środowisku pracy biurowej. Klient nie troszczy się o system operacyjny, lecz może swobodnie pisać aplikacje, albo korzystać ze środowiska flowchart.
IaaS (Infrastructure As Service) – najbardziej zaawansowany model usług Cloud Computing polegający na dostarczeniu całej zwirtualizowanej infrastruktury teleinformatycznej, rozbudowywanej w zależności od potrzeb. Jeśli klient dostarczy dostawcy swoje oprogramowanie do instalacji na zwirtualizowanym sprzęcie, usługa ta nosi nazwę HaaS (Host As Service).

2. Omówienie poszczególnych rang zagrożeń

a. Nadużycie i użycie w celu przestępczym Cloud Computing

Wpływ: organizacje kryminalne działające w Internecie wprowadzają nowe technologie w celu uniknięcia wykrycia i zwiększenia efektywności swoich działań. Ze względu na relatywnie słabe systemy rejestracji zapewniające anonimowość i ograniczające możliwości wykrycia oszustwa, systemy Cloud Computing mogą stanowić dla nich ważny cel ataków.

Zagrożenie: IaaS (Infrastructure As Service), Paas (Platfrom As Service)

Opis: Firmy IaaS oferują użytkownikom nieograniczoną moc przetwarzania, pasma sieci i miejsca na składowanie danych. Jest to po trosze trick reklamowy mający przyciągnąć klientów, bowiem w zamian za to spada bezpieczeństwo. Sam proces rejestracji bowiem ogranicza się wyłącznie do sprawdzenia statusu karty płatniczej, na podstawie czego użytkownik od razu może zyskać dostęp do zamówionych usług. Niektóre firmy wręcz wprowadzają okres wolny od opłat (trial) i rejestrowanie na podstawie danych firmy lub osobowych. Spamerzy, autorzy złośliwego kodu i inni cyberkryminaliści, nadużywając tej relatywnej anonimowości, stojącej za rejestracją i procesem użytkowania, mogą prowadzić swoją aktywność w warunkach relatywnej bezkarności. Pola ich działań to głównie prowadzenie zdalnie ataków DDOS, kradzież haseł i kluczy, ich rozłamywanie, przechowywanie złośliwego kodu, budowa centrów kierowania dla botnetów oraz aplikacji omijających kody CAPTCHA Największe straty z tytułu tego zagrożenia mogą ponieść firmy prowadzące usługi PaaS. Jak wykazują raporty firm bezpieczeństwa zagrożone są także firmy IaaS.

Przykłady: firmy IaaS zmniejszając bezpieczeństwo umożliwiają dostęp do botnetów Zeus, koni trojańskich InfoStealer, oraz mechanizmów ściągania dla exploitów Microsoft Office i Adobe PDF. Dodatkowo usługi oferowane przez IaaS wykorzystywane są do tworzenia zdalnych centrów kontroli dla botnetów. Spam jest też problemem – całe bloki adresów firm IaaS znajdują się na czarnych listach antyspamowych.

Środki zaradcze:

- początkowa rejestracja i walidacja użytkowników nie powinny być tak łatwe
- Konieczne jest poprawienie skuteczności mechanizmów wykrywania oszustw kart płatniczych
- Niezbędna jest obserwacja ruchu w usługach klientów
- Niezbędne jest monitorowanie czarnych list dla stwierdzenia czy przypadkiem nie znajdują się na nich firmowe adresy

b. Niebezpieczne interfejsy i API

Wpływ: Większość firm dąży do zapewnienia bezpieczeństwa integrując je w swoich modelach usług – także w ich interfejsach. Konieczne jest zrozumienie, jaka jest różnica między tym modelem, a modelem obejmującym zarządzanie i koordynację usług w chmurze. Słabe zabezpieczenie interfejsów i API wystawia organizację na szereg ryzyk powiązanych z poufnością, integralnością, dostępnością i odpowiedzialnością.

Zagrożenie: IaaS, PaaS, SaaS (Software As Service)

Opis: Firmy dostępu Cloud Computing wystawiają w Sieci interfejsy oprogramowania albo API. Są one wykorzystywane do tworzenia interakcji z usługami chmury lub zarządzania nimi. Zabezpieczenie tych najważniejszych API jest krytyczne, bo to od nich zależy bezpieczeństwo i dostępność podstawowych usług w chmurze.
Interfejsy muszą być tak wykonane, aby zabezpieczały przed zarówno przypadkowym jak i intencjonalnym łamaniem polityk bezpieczeństwa. Wachlarz stosowanych w ich przypadku środków musi obejmować jak najwięcej funkcjonalności bezpieczeństwa od autentykacji i kontroli dostępu do szyfrowania i monitorowania aktywności.
Ważne jest, że organizacje i trzecie strony często tworzą interfejsy i API, aby zaoferować wartość dodaną do usług swoim klientom. W tym momencie wychodzi na jaw złożoność nowego wielowarstwowego API - ryzyko dla bezpieczeństwa znacznie wzrasta, jeśli jego użycie wprowadza rozwiązania na mocy których organizacja jest zobowiązana do zrzeczenia się choćby części swoich praw na rzecz strony trzeciej. Dzieje się tak zwykle po wejściu w życie umowy wprowadzającej dodatkowego agenta między usługodawcą a klientem.

Przykłady: Niewłaściwe działania pogarszające bezpieczeństwo interfejsów i API, to zwykle: dostęp anonimowy i powtórne używanie tokenów lub haseł, autentykacja przy użyciu czystego tekstu lub transmisja contentu, nieelastyczny system kontroli dostępu lub niewłaściwa autoryzacja, ograniczone możliwości monitoringu lub sprawdzania logów, wprowadzanie nieznanych usług lub zależności API.

Środki zaradcze:

- analiza modelu bezpieczeństwa interfejsu dostępowego usługodawcy dostępu do chmury
- Wprowadzenie mocnej autentykacji i kontroli dostępu razem z szyfrowaniem transmisji
- Rozpoznanie łańcucha zależności związanego z API

c. Wrogie działania wewnątrz chmury

Wpływ: Jeśli osoby znajdujące się wewnątrz firm-usługodawców podejmą wrogie działania, ich negatywny wpływ może być znaczny, jako że najczęściej mają one nieskrępowany dostęp do klientów i ich aktywów. Niszczenie marki, straty finansowe i produktywności - to tylko część szkód, jakie można ponieść na skutek ich działalności. Wbrew pozorom bowiem, w momencie przejęcia przez firmę modelu Cloud Computing, czynnik ludzki jeszcze bardziej zyskuje na znaczeniu. Klienci muszą wobec tego mieć pewność, że dostawcy usług w chmurze zabezpieczyli się przed tego typu zagrożeniem w sposób co najmniej dostateczny

Zagrożenia: IaaS, PaaS, SaaS.

Opis: Zagrożenie działaniami wrogimi z wewnątrz firmy jest dobrze znane wielu organizacjom. Dla klientów usług w chmurze wzrasta ono w znacznym stopniu, , ponieważ następuje konwergencja tych usług i usług klienta i są one zarządzane w jednej domenie. Samo zagrożenie wynika zaś z generalnego niedostatku przejrzystości w procesie i procedurach dostępu
Dla przykładu firma dostępowa może nie ujawnić w jaki sposób przydzielany jest pracownikom dostęp do zasobów fizycznych i wirtualnych. Zwykle nie ujawnia też jak monitorowani są ci pracownicy i w jaki sposób następuje raportowanie dotyczące zachowania polityk. Ten rodzaj postępowania tworzy dogodne pole dla działania kilku typów aktywności kryminalnej: hackera-hobbysty, przestępcy, przestępcy działającego w organizacji, szpiegostwa korporacyjnego a nawet ataku sponsorowanego przez agendę innego państwa. Uzyskanie wysokiego poziomu dostępu w takich okolicznościach umożliwia zebranie poufnych danych lub uzyskanie kompletnej kontroli nad usługami określonej firmy bez ryzyka wykrycia i zdemaskowania.

Przykłady:
Jak podejrzewali analitycy i później udowodniło śledztwo prowadzone przez FBI, za atakami na konta Google przeprowadzonymi w dwóch seriach zimą i wiosną 2010 roku, stały osoby zarówno z zewnątrz jak i z wewnątrz firmy. Jednak sprawdziły się ostrzeżenia analityków, że wroga aktywność wewnątrz firmy jest trudna nie tylko do wykrycia, ale i do udowodnienia. Przeciwko trzem pracującym w Google specjalistom IT oskarżonym o wspomaganie hackerów działających z Chin nie zgromadzono dostatecznych dowodów, aby można było postawić ich w stan oskarżenia. Skończyło się na zwolnieniu bądź zawieszeniu managementu całego działu Azji i Pacyfiku przez zarząd firmy.
Środki zaradcze:

- Wprowadzenie rozwiązania wspomagania zarządzania zasobami SCM oraz kompleksowej oceny dostawców
- Określenie warunków zarządzania zasobami ludzkimi w części prawnej kontraktu
- Wprowadzenie przejrzystości do całości bezpieczeństwa informatycznego i działań managementu podobnie jak raportowanie zgodności
- Określenie procesu powiadamiania o łamaniu bezpieczeństwa.

d. Luki w aplikacjach i mechanizmach Shared Technology

Wpływ: Ataki prowadzone w ostatnich latach obejmują coraz częściej mechanizmy Shared Technology w usługach Cloud Computing. Partycje dysku, procesory (cache), procesory kart graficznych inne elementy służące wymianie danych nigdy nie były konstruowane pod kątem dzielenia zasobów i wymiany danych. W rezultacie, praca w tym trybie jest często ich piętą Achillesową, a ataki – dość łatwe do przeprowadzenia. Po przeprowadzeniu takiego skutecznego ataku hackerzy mogą skoncentrować się na operacjach przeciwko klientom Cloud Computing i sposobie uzyskania nieautoryzowanego dostępu do ich danych.

Zagrożenia: IaaS

Opis: Prowadzący IaaS dostarczają swoje usługi w sposób skalowalny poprzez infrastrukturę służącą wymianie. Często, komponenty tworzące tę infrastrukturę (cache CPU, GPU i inne) nie były zaprojektowane do oferowania zabezpieczonych funkcjonalności w architekturze, w której w tym samym czasie działa jednocześnie wielu klientów. Jest to słaby punkt infrastruktury Cloud Computing. Firmy oferujące usługi i infrastrukturę w chmurze, próbują zabezpieczyć się przed wykorzystaniem tej luki, wprowadzając hiperwizora usług wirtualizacji, który mediuje pomiędzy operacyjnym systemem gościa wykorzystującego usługę a fizyczna warstwą sprzętową. Jednak, o ile wprowadzenie takiego oprogramowania powoduje widoczną poprawę zarządzania zasobami, o tyle nie likwiduje do końca luk bezpieczeństwa sprzętowego. Ich wykorzystanie umożliwia systemowi operacyjnemu gościa uzyskanie niewłaściwego poziomu kontroli lub wpływu na platformy niskiego poziomu (sprzętowe).
W tej sytuacji dla zabezpieczenia się przed takimi działaniami konieczne jest stworzenie mechanizmu silnej wymiany, by klienci indywidualni nie włamywali się w operacje innych działających w tej samej chmurze. Klienci nie powinni mieć możliwości uzyskania dostępu do jakichkolwiek danych bądź zasobów, ruchu sieciowego itp. należących do innych użytkowników. W tym celu także ważne jest stworzenie strategii głębokiej obrony, zawierającej zarządzanie przetwarzaniem, przechowywaniem, ochroną bezpieczeństwa sieci i jej monitoringiem.

Przykłady: Najbardziej znanymi i do tej pory nie załatanymi mechanizmami wykorzystania luk sprzętowych są Red i Blue Pill Joanny Rutkowskiej oraz CloudBurst Aleksandra Korczinskiego

Środki zaradcze:

- wprowadzenie najlepszych praktyk dotyczących instalacji i konfiguracji
- Monitorowanie środowiska dla zmian lub aktywności nieautoryzowanej
- Promowanie silnej autentykacji i kontroli dostępu dla operacji i dostępu na poziomie administratora
- Wymuszenie w SLA uaktualniania i zaradzania lukom
- Wprowadzenie audytów skanowania i konfiguracji wykazywania luk

e. Wycieki lub utrata danych

Wpływ: Utrata lub wyciek danych może zniszczyć firmę i biznes. Poza bezpośrednimi naruszeniami marki i reputacji, mają one znaczący wpływ na morale i zaufanie pracowników, partnerów i klientów. Utrata najważniejszej części własności intelektualnej może mieć implikacje zarówno finansowe jak i konkurencyjne. Co gorsza, jeśli firma opiera się na danych, które mogły zostać utracone lub wyciekły, może spodziewać się naruszenia ich zgodności lub późniejszych konsekwencji prawnych

Zagrożenia: IaaS, PaaS, SaaS

Opis: Istnieje wiele sposobów na nielegalne uzyskanie dostępu bądź zniszczenie danych. Jednym z często spotykanych przykładów jest skasowanie lub nadpisanie zapisów bez backupu oryginalnej zawartości. Innym jest nie połączenie pojedynczego zapisu z większym zbiorem to którego on należy. Może to uczynić zapis nieodzyskiwalnym tak samo jak przechowywanie danych na niedostępnym nośniku. Destrukcyjny rezultat może mieć także utrata klucza szyfrującego.

Warto pamiętać, że zagrożenie uzyskaniem dostępu bądź zniszczeniem danych rośnie w przypadku Cloud Computing, z powodu wzrostu ilości interakcji pomiędzy ryzykami. Część z nich jest bowiem charakterystyczna tylko dla przetwarzania w chmurze. Bardziej niebezpieczne są też charakterystyki operacyjne bądź architektury Cloud Computing niż klasycznej systemowej. W tej sytuacji istotne jest uniemożliwienie nieautoryzowanego dostępu do wrażliwych danych.

Przykłady: Najczęstsze „grzechy" w przypadku tego typu zagrożeń to: niedostateczna autentykacja, autoryzacja i kontrola audytu (system AAA), niespójne użycie kluczy szyfrujących i programowych, błędy proceduralne.
Istnieją też problemy trwałe i chwilowe związane z Cloud Computing, jak:

- rozproszenie działań w pracy Cloud Computing,
- ryzyko połączeń, ryzyko polityczne i nadzoru prawnego,
- kwestia niezawodności centrów danych
- działanie systemu przywracania po awarii

Środki zaradcze:

- wprowadzenie mocnej kontroli dostępu API
- szyfrowanie i ochrona integralności przekazu
- Analiza ochrony danych zarówno w czasie obróbki jak i tworzenia
- Wprowadzenie silnych kluczy, przechowywania i zarządzania i polityk niszczenia danych
- Umowne żądanie czyszczenia używanych wcześniej mediów przez dostawców usług Cloud przed powtórnym wprowadzeniem ich do obrotu
- Umowne wyspecyfikowanie polityki backupu i retencji danych u dostawców usług Cloud.

f. Przechwycenie usługi, ruchu lub konta

Wpływ: Jednym z głównych zagrożeń jakiegokolwiek typu przetwarzania danych pozostaje przechwycenie konta lub usługi, zwykle przy użyciu skradzionych uwierzytelnień. . Za pomocą skradzionych uwierzytelnień hackerzy bardzo często uzyskują dostęp do krytycznych obszarów wystawionych usług Cloud Computing. Umożliwia to im przejęcie bądź zniszczenie poufności, integralności i dostępności tych usług. Konieczne jest zabezpieczenie przed tego typu atakami – zarówno za pomocą strategii wysuniętej obrony zakładającej prewencyjne monitorowanie ruchu i nawet nadzór nad klientami, jak i przy pomocy klasycznych zabezpieczeń biernych (firewalle, labirynty, fałszywe konta itp.). Przeciwdziała to zniszczeniom (i możliwym sporom) będącym skutkami przechwyceń.

Zagrożenia: IaaS, PaaS, SaaS

Opis: Tego typu ataki nie są niczym nowym. Ciągle jeszcze przynosi rezultaty używanie w nich phishingu, oszustwa czy exploitów programowych dla wykorzystania luk.. Uwierzytelnienia i hasła zwykle są powtórnie używane, co wspomaga siłę tych ataków. Usługi Cloud Computing dodają nowe zagrożenia do już istniejących w tej klasie bezpieczeństwa. Jeśli atakujący otrzyma bowiem dostęp do uwierzytelnień, może podsłuchiwać i odnotowywać każdy ślad aktywności i transakcji, manipulować danymi, fałszować informacje zwrotne i przekierowywać klientów do zagrażających im stron. Konto i

usługi w chmurze mogą stać się nowa bazą dla atakującego. Działając z niej może znacznie osłabić reputacje usługodawcy.

Przykłady: Przejęcie kont lub usług jest wymieniane w kontekście pojedynczych przypadków Cloud Computing, ale – co zrozumiałe – żaden z usługodawców IaaS, PaaS czy SaaS nie chce potwierdzić, że w jego przypadku takie zdarzenie rzeczywiście miało miejsce.

Środki zaradcze:

- zabezpieczenie przed wymianą kont i usług między użytkownikami
- Wprowadzenie silnej autentykacji dwuskładnikowej tam, gdzie jest to możliwe
- Wprowadzenie monitoringu proaktywnego dla wykrywania nieautoryzowanego dostępu
- Ustalenie, jakie są polityki i SLA dostawcy usług w chmurze.

g. Ryzyko nieznanego poziomu

Wpływ: Kiedy zostają wprowadzone usługi Cloud Computing, funkcjonalności i funkcje muszą być dobrze adresowane – i tak się zwykle staje. Co jednak dzieje się z wewnętrznymi procedurami bezpieczeństwa, zmianami konfiguracji w kierunku jej umocnienia, uaktualnianiem, wprowadzaniem łat, audytowaniem i logowaniem? Gdzie umieszczone są dane i powiązane z nimi logi i kto ma do nich dostęp? Jakie informacje ujawnia usługodawca w wypadku incydentu bezpieczeństwa? Kwestie te zwykle nie są jasno określone lub nawet pomijane zarówno w negocjacjach dotyczących usług jak i samych umowach. Zostawia to klientów z perspektywą ryzyka nieznanego stopnia, które może zawierać rzeczywiste poważne zagrożenia

Zagrożenia: IaaS, PaaS, SaaS

Opis: Jednym z dogmatów pracy w chmurze jest redukcja posiadanego sprzętu i oprogramowania oraz kosztów utrzymania co pozwala firmom skupić się na umocnieniu core business.
Teoretycznie oznacza to same zyski – zwłaszcza w obszarze finansowym i operacyjnym. Popularność usług Cloud Computing wynika zbyt często z dość rudymentarnych wyliczeń określających ile firma może zaoszczędzić na ich wprowadzeniu. Ale tak naprawdę przy tym wyliczaniu nie uwzględnia się ryzyk bezpieczeństwa.
Aby je obliczyć potrzebne są tak istotne informacje o infrastrukturze i praktykach działania z nią jak: istniejące w firmie wersje software, praktyki uaktualniania kodu, bezpieczeństwa, profile zagrożeń, systemy działania przeciw atakom i projektowania bezpieczeństwa.
Ważnym dodatkiem do danych jednostkowych bezpieczeństwa jak logi ataków, przekierowań i logi innego typu mogą być także informacje, kto korzysta z infrastruktury.

Przykłady: Konflikt IRS – Amazon, kiedy ten urząd podatkowy zarządzał danych użytkowników Amazon, zaś portal odmówił.
Heartland Data Breach: system płatności Heartland używał dobrze znanego, wrażliwego na ataki i zainfekowanego już oprogramowania, ale Heartland stwierdził iż spełni tylko minimalne uwymagania stawowe czyli w praktyce jedynie powiadomi klienta czy jego dane nie zostały skradzione.

Środki zaradcze:

- Ujawnienie zastosowania logów i danych

- Częściowe lub pełne ujawnienie detali infrastruktury
- Monitorowanie i alarmowanie przy niezbędnych informacjach.

Marek Mejssner