Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu

Bezpieczne korzystanie z chmury

REDAKTOR GOŚCINNY

James Tarala jest redaktorem gościnnym tego wydania. James jest starszym instruktorem w SANS Institute oraz głównym konsultantem w Enclave Security. Jest także autorem licznych szkoleń SANS, w tym audytu SANS 566: Wdrażanie i audyt dwudziestu krytycznych punktów kontroli bezpieczeństwa oraz audytu SANS 407: Podstawy przeprowadzania audytów systemów informacyjnych.

WSTĘP

Usługi w chmurze to zaawansowana technologia chętnie adaptowana przez wiele podmiotów i organizacji. Chmura obliczeniowa (tzw. cloud computing) jest w istocie niczym więcej niż powierzeniem składowania i zarządzania swoimi danymi dostawcy usług. Powodem dla którego nazywamy tę usługę "chmura" to fakt, że nigdy nie wiadomo gdzie dokładnie dane są fizycznie przechowywane - jest to obsługiwane przez "chmurę". Przykładami powszechnie znanych usług w chmurze są dokumeny na Google Docs, udostępnianie plików przez Dropbox, uruchamianie własnego serwera na Amazon Elastic Compute Cloud czy przechowywanie muzyki i zdjęć na iCloud Apple. Dzięki takim usługom online praca może być dużo bardziej produktywna, jednak wraz z ich wszystkimi zaletami i szerokimi możliwościami może pojawić się ryzyko. W biuletynie przyjrzymy się potencjalnym problemom z tym związanym i omówimy jak można chronić swoje informacje.

WYBÓR DOSTAWCY USŁUG

Nie można jednoznacznie stwierdzić, że chmura jest rozwiązaniem dobrym albo złym, jest to po prostu narzędzie do wykonania zadań, zarówno w pracy jak i w domu. Jednak korzystając z niej powierzasz bezpieczeństwo swoich osobistych danych nieznanym podmiotom. Wówczas należy upewnić się, że spełniają one pewne wymagania. Warto wziąć pod uwagę zadanie następujących pytań podczas poszukiwania dostawcy usług w chmurze:

1. **Wsparcie.** Jak szybkie wsparcie oferowane jest przez firmę w przypadku kiedy masz problem z usługą? Gdy dane są krytyczne, może być wymagana pomoc telefoniczna lub mailowa. Jeśli firma nie zapewnia takiego wsparcia, czy firma na swojej stronie internetowej posiada publiczne forum lub sekcję FAQ (ang. Frequently Asked Questions - często zadawane pytania)?
2. **Kopie zapasowe.** Czy firma tworzy kopię zapasową Twoich danych? Jeśli tak, to co dokładnie się w niej znajduje, jak często jest robiona i jak długo kopie zapasowe są przechowywane? Czy w wypadku przypadkowego usunięcia plików, możesz je odzyskać, a jeśli tak, to jak?
3. **Prywatność.** Komu dostawca usług w chmurze zezwala na dostęp do Twoich danych? Czy dostęp masz tylko Ty czy także pracownicy dostawcy lub podmioty trzecie, np. partnerzy dostawcy?

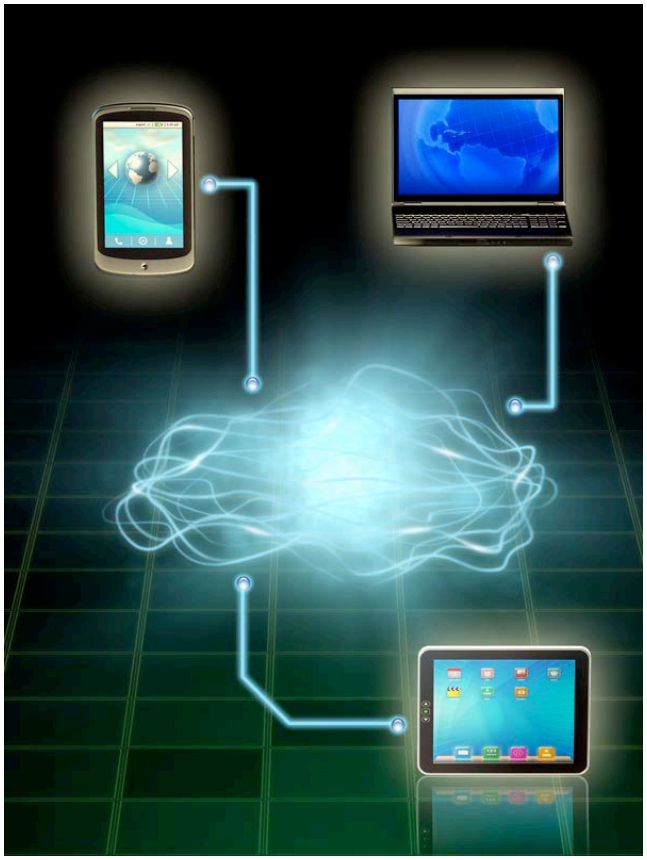
Bezpieczne korzystanie z chmury

4. **Bezpieczeństwo.** Jak Twoje dane są przesyłane z komputera lub urządzenia do chmury? Czy połączenie jest zabezpieczone szyfrowaniem? Jak przechowywane są Twoje dane w chmurze, czy są po raz kolejny szyfrowane? Kto może odszyfrować dane?

BEZPIECZNY DOSTĘP

Po wybraniu firmy do przechowywania danych w chmurze, następnym krokiem jest upewnienie się, że korzysta się z jej usług prawidłowo. To w jaki sposób uzyskuje się dostęp do danych oraz jak się nimi dzieli może mieć o wiele większy wpływ na bezpieczeństwo danych niż cokolwiek innego. Kluczowe kroki jakie można podjąć, aby chronić swoje dane obejmują:

1. **Uwierzytelnianie:** Używaj silnych, długich kombinacji znaków do uwierzytelnienia się u dostawcy usług w chmurze. To uchroni przed atakami mającymi na celu odgadnięcie hasła. Jeśli Twój dostawca oferuje dwustopniowe uwierzytelnianie (czasami nazywane dwustopniową weryfikacją), zaleca się go używać.
2. **Udostępnianie:** Usługi w chmurze sprawiają, że wymiana danych stała się bardzo prosta, należy uważać, aby przypadkiem nie udostępnić innym zbyt dużo danych. W najgorszym przypadku, można niechcący udostępnić swoje dane publicznie. Najlepszym sposobem zabezpieczenia się jest domyślne ustawienie aby nie udostępniać żadnych danych nikomu. Wówczas pozwolić tylko konkretnym osobom (lub grupom osób) na dostęp do określonych plików lub folderów z niezbędnymi informacjami.
3. **Ustawienia:** Poświęć chwilę aby dobrze zrozumieć ustawienia zabezpieczeń oferowanych przez operatora chmury. Czy jeśli przyznasz pełną kontrolę komuś innemu, może on z kolei udostępnić Twoje dane osobom trzecim bez Twojej wiedzy i zgody? Czy możesz całkowicie usunąć swoje dane od dostawcy kiedy nie potrzebujesz więcej korzystać z usługi?



Chmura obliczeniowa może pomóc zaoszczędzić pieniądze i zwiększyć produktywność, jednak należy uważać na to jak przechowujesz i udostępniasz informacje.

4. **Antywirus:** Upewnij się, że najnowsza wersja oprogramowania antywirusowego jest zainstalowana na każdym komputerze służącym do korzystania z chmury i dzielenia się swoimi danymi. Jeżeli plik który udostępniasz zostaje zainfekowany, inne komputery mające dostęp do tego samego pliku mogą się również zarazić.
5. **Szyfrowanie:** W jaki sposób Twój dostawca szyfruje dane? Czy to on kontroluje klucze czy Ty? Solidnym sposobem zabezpieczeń jest szyfrowanie

Bezpieczne korzystanie z chmury

swoich prywatnych danych lokalnie przed ich przesłaniem do chmury. Ten dodatkowy krok chroni dane nawet jeśli serwer dostawcy usługi zostanie skompromitowany.

6. **Backup:** Nawet jeśli Twój dostawca tworzy kopie zapasowe danych, warto zaplanować regularne tworzenie własnych, lokalnych kopii zapasowych. To nie tylko ochroni Twoje dane nie tylko na wypadek zniknięcia usługodawcy, ale także sprawi że łatwiej będzie odzyskać duże ilości danych z lokalnej kopii zapasowej niż ściągać je z chmury.
7. **Regulamin:** Czytaj dokładnie umowy o warunkach świadczenia usług i licencji - Service Level Agreement (SLA) i End User License Agreement (EULA) - przed zapisaniem się do usługi. Rozważ podpisanie umowy z innymi dostawcami, jeśli istnieją warunki w umowie, których nie rozumiesz lub które Cię niepokoją.
8. **Dane organizacyjne:** Nie przechowuj danych organizacji w chmurze bez uzyskania uprzedniej zgody przełożonego. Przechowywanie danych organizacji w chmurze może nie tylko naruszyć zasady obowiązujące w organizacji, ale także naruszać prawa obowiązujące w danym kraju, narażając Ciebie i Twoją organizację na prawne konsekwencje.

PODSUMOWANIE

Chmura nie jest ani dobrem ani złem, to po prostu narzędzie którym można się posłużyć. Najważniejsze kroki do własnej ochrony to wybór właściwego dostawcy usług i właściwa kontrola tego w jaki sposób uzyskujesz dostęp do danych i jak się nimi dzielisz.

ŹRÓDŁA

W celu poprawy czytelności tekstu niektóre odnośniki w biuletynie zostały skrócone przy użyciu usługi TinyURL. Dla zachowania bezpieczeństwa, OUCH! używa funkcji podglądu TinyURL, która pozwala podejrzeć docelowy adres odnośnika oraz pyta o pozwolenie przed wejściem na stronę o docelowym adresie.

The Cloud Security Alliance (CSA):
https://cloudsecurityalliance.org

Słownik pojęć bezpieczeństwa:
http://preview.tinyurl.com/6wkpae5

Porada dnia SANS Security:
http://preview.tinyurl.com/6s2wrkp

DOWIEDZ SIĘ WIĘCEJ

Zasubskrybuj comiesięczny Biuletyn Bezpieczeństwa Komputerowego – SANS OUCH! Zdobądź dostęp do archiwów i poznaj rozwiązania SANS z zakresu bezpieczeństwa komputerowego i osobowego. Odwiedź http://www.securingthehuman.org i dowiedz się więcej.

POLSKI PRZEKŁAD

CERT Polska jest zespołem działającym w strukturach NASK powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w polskiej sieci Internet.
Należy do organizacji FIRST, w ramach której współpracuje z podobnymi zespołami na całym świecie.
WWW: http://www.cert.pl
Twitter: @CERT_Polska
Facebook: http://facebook.com/CERT.Polska

Redakcja: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner
Polski przekład (NASK/CERT Polska): Katarzyna Gorzelak, Paweł Jacewicz