OUCH! | Listopad 2016

Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu..

Bezpieczne korzystanie z chmury

Wstęp

Nazwa “Chmura” (cloud) może być wieloznaczna ale w istocie jest niczym więcej niż powierzeniem składowania i zarządzania swoimi danymi dostawcy takich usług za Ciebie. Zaletą chmury jest łatwy dostęp i synchronizacja naszych danych na wielu urządzeniach znajdujących sie w dowolnym miejscu na świecie, a także możliwość łatwego dzielenia się tymi danymi z innymi osobami. Powodem dla którego nazywamy tę usługę „chmura” jest fakt, że nigdy nie wiadomo gdzie dokładnie dane są fizycznie przechowywane. Przykładami popularnych czynności wykonywanych w chmurze jest tworzenie dokumentów na Google Docs, udostępnianie plików przez Dropbox, uruchamianie własnego serwera na Amazon Cloud czy przechowywanie muzyki i zdjęć na iCloud Apple. Dzięki tego typu usługom online, praca może być dużo bardziej wydajna, jednak wraz ze wszystkimi zaletami i szerokimi możliwościami może pojawić się pewne ryzyko. W tym biuletynie opiszemy jak bezpiecznie korzystać z chmury.

Redaktor gościnny

Dave Shackleford (**@daveshackleford**) jest profesjonalnym konsultantem, właścicielem Voodoo Security oraz autorem licznym kursów wydawanych przez SANS, włącznie z SANS Security 579, Wirtualizacja, Ochrona Prywatnej Chmury i Bezpieczeństwo 524 oraz Podstawy Bezpieczeństa Chmury.

Wybór dostawcy usług w chmurze

Nie można jednoznacznie stwierdzić, że chmura jest rozwiązaniem dobrym albo złym, jest po prostu narzędziem do wykonywania zadań, zarówno w pracy jak i w domu. Jednak korzystając z niej powierzasz swoje osobiste dane osobom nieznanym oczekując, że będą zarówno bezpieczne jak i łatwo dostępne. Dlatego musisz być pewien, że dokonujesz właściwego wyboru dostawcy usług. W kwestii komputerów służbwych lub urządzeń zawierających informacje służbowe, skontaktuj się z przełożonym i dowiedz czy możesz korzystać z usług w chmurze. Jeśli tak, pamiętaj, aby potwierdzić z których dokładnie usług w chmurze można korzystać i jakie regulaminy tam obowiązują. Jeśli szukasz usług w chmurze do użytku osobistego, weź pod uwagę następujące kwestie:

1. **Wsparcie**: Jak szybko otrzymasz pomoc lub odpowiedź na pytanie w przypadku, kiedy masz problem z usługą? Czy jest podany numer telefonu albo adres email, poprzez które możesz się skontaktować z dostawcą? Czy firma na swojej stronie internetowej posiada inne rodzaje wsparcia, takie jak publiczne forum lub sekcję FAQ (ang. Frequently Asked Questions - często zadawane pytania)?
2. **Prostota**: Jak łatwo jest korzystać z usługi? Im bardziej skomplikowane jest korzystanie z niej, tym bardziej prawdopodobne, że będziesz popełniać błędy i przypadkowo narazisz się na utratę lub ujawnienie swoich danych. Skorzystaj z serwisu

Bezpieczne korzystanie z chmury

dostawcy chmury który można łatwo zrozumieć, skonfigurować i używać.

3. **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? A jeśli tak to kto może odszyfrować dane?
4. **Regulamin korzystania z usługi**: Poświęć chwilę, aby przejrzeć regulamin (zwykle są pisane bardzo przystępnym językiem). Potwierdź, kto może uzyskać dostęp do Twoich danych i jakie są Twoje prawa.

Chmura może sprawić, że Twoje dane będą łatwiej dostępne i pomoże zwiększyć produktywność. Jednak uważaj na to, jak przechowujesz i udostępniasz swoje informacje.

Zabezpiecz swoje dane

Po wybraniu firmy której powierzysz przechowywanie danych w chmurze, następnym krokiem jest upewnienie się, że korzystasz 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 ich bezpieczeństwo niż cokolwiek innego. Kluczowe kroki jakie można podjąć, aby chronić swoje dane obejmują:

1. **Uwierzytelnianie**: Używaj silnych, unikalnych kombinacji znaków do uwierzytelnienia się u dostawcy usług w chmurze. Jeśli Twój dostawca oferuje dwustopniowe uwierzytelnianie (czasami nazywane dwustopniową weryfikacją), zaleca się go używać.
2. **Udostępnianie plików i folderów**: Usługi w chmurze sprawiają, że wymiana danych stała się bardzo prosta, czasem może nawet zbyt prosta. Czarny scenariusz dla korzystającego z chmury to przypadkowe udostępnienie plików lub całych katalogów publicznie. Najlepszym sposobem zabezpieczenia się jest domyślne ustawienie aby nie udostępniać żadnych danych nikomu. Wówczas nadasz uprawnienia tylko konkretnym osobom (lub grupom osób) na dostęp do określonych plików lub folderów. Jeśli taka osoba nie będzie już potrzebowała dostępu do Twoich plików, należy go usunąć. Dostawca usług w chmurze powinien zapewnić łatwy sposób na monitorowanie kto ma dostęp do takich danych.
3. **Udostępnianie plików/folderów za pomocą linków**: Popularną funkcją niektórych usług w chmurze jest zdolność do tworzenia specjalnego linku, który wskazuje na twoje pliki i foldery. Ta funkcja pozwala na udostępnianie tych plików komukolwiek tylko za pomocą podania mu adresu. Jednak takie podejście nie cechuje się wysokim poziomem bezpieczeństwa bo każdy, kto zna ten link może uzyskać dostęp do twoich osobistych plików lub folderów. Jeśli wyślesz link do tylko jednej osoby, może ona udostępnić ten link innym lub może on pojawić się w wyszukiwarkach. Jeśli zdecydujesz się na udostępnianie danych przy użyciu linku internetowego, należy wyłączyć link kiedy nie jest już potrzebny lub, jeśli to możliwe, zabezpieczyć go hasłem.

Bezpieczne korzystanie z chmury

4. **Ustawienia**: Poświęć chwilę aby dobrze zrozumieć ustawienia zabezpieczeń oferowanych przez operatora chmury. Na przykład, czy jeśli przyznasz komuś uprawnienia do folderu, może on z kolei udostępnić te dane osobom trzecim bez Twojej wiedzy i zgody? Warto też sprawdzić czy jest możliwość obserwowania kto może oglądać udostępniane pliki i kiedy to robi. Czy możesz ustawić opcję "tylko do odczytu" zamiast "pisanie/czytanie", która oznacza, że ludzie będą mogli także modyfikować pliki?
5. **Antywirus**: Upewnij się, że najnowsza wersja oprogramowania antywirusowego jest zainstalowana na Twoim komputerze i na każdym innym komputerze wykorzystywanym do dzielenia się swoimi danymi. Jeżeli plik który udostępniasz zostaje zainfekowany, inne komputery mające dostęp do tego samego pliku mogą się również zarazić.

Dowiedz się więcej

Zasubskrybuj comiesięczny biuletyn o bezpieczeństwie komputerowym SANS OUCH! Zdobądź dostęp do archiwów i poznaj rozwiązania SANS dotyczące bezpieczeństwa komputerowego i osobowego.
Odwiedź securingthehuman.sans.org/ouch/archives 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

Źródła

Dwuskładnikowe uwierzytelnianie:	https://securingthehuman.sans.org/ouch/2015#september2015
Nowe oblicze hasła:	https://securingthehuman.sans.org/ouch/2015#april2015
Menedżery haseł:	https://securingthehuman.sans.org/ouch/2015#october2015
Czym jest złośliwe oprogramowanie:	https://securingthehuman.sans.org/ouch/2016#march2016
SEC524: Cloud Security Fundamentals:	https://sans.org/sec524

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Polski przekład (NASK/CERT Polska): Małgorzata Dębska, Przemysław Zielony, Sebastian Kondraszuk

