OUCH! Sierpień 2021

SANS SECURITY AWARENESS

OUCH!

Biuletyn Bezpieczeństwa Komputerowego

Bezpieczne przechowywanie danych w chmurze

Wstęp

Być może obiła Ci się o uszy koncepcja zwana "chmurą". Nazwa ta może być wieloznaczna, ale w istocie jest niczym więcej niż miejscem w sieci, w którym są przechowywane i zarządzane dane przez dostawcę usługi. Przykłady obejmują tworzenie dokumentów w usłudze Google Docs, dostęp do poczty Microsoft O365, udostępnianie plików za pośrednictwem usługi Dropbox czy też przechowywanie zdjęć w usłudze iCloud firmy Apple. Zaletą chmury jest łatwy dostęp i synchronizacja danych na wielu urządzeniach znajdujących się w dowolnym miejscu na świecie, a także możliwość łatwego dzielenia się nimi z innymi osobami.

Wybór dostawcy usług w chmurze

Nie można jednoznacznie stwierdzić, że chmura jest rozwiązaniem dobrym czy złym. Chmury po prostu są narzędziami do wykonywania zadań, zarówno w domu jak i w pracy. Jednak korzystając z tego rozwiązania, powierzasz swoje dane osobiste obcym osobom i oczekujesz, że będą one zarówno bezpiecznie jak i łatwo dostępne w każdym momencie. Dlatego musisz mieć pewność, że dokonujesz właściwego wyboru dostawcy usług. W kwestii danych służbowych, skontaktuj się z przełożonym i dowiedz się, czy dane firmowe mogą być przechowywane w chmurze. Jeśli zastanawiasz się nad korzystaniem z tego typu usług do użytku osobistego, rozważ następujące kwestie:

1. **Zaufanie**: Czy możesz zaufać dostawcy usługi? Czy jest to dobrze znana firma, z której usług korzystają miliony ludzi, czy też mała, nieznana firma z siedzibą w kraju, o którym nigdy nie słyszałeś?
2. **Wsparcie**: Jak szybko otrzymasz pomoc lub odpowiedź na pytanie? Czy jest podany numer telefonu albo adres e-mail, poprzez które możesz skontaktować się z dostawcą? Czy firma na swojej stronie internetowej posiada inne rodzaje wsparcia, takie jak publiczne forum czy sekcję FAQ (ang. Frequently Asked Questions - często zadawane pytania)?
3. **Prostota**: Jak łatwo jest korzystać z usługi? Im bardziej skomplikowane jest korzystanie z niej, tym bardziej prawdopodobne jest, że będziesz popełniać błędy i przypadkowo narazisz się na utratę lub ujawnienie swoich danych. Korzystaj z serwisu dostawcy chmury, który można łatwo zrozumieć, skonfigurować oraz używać.
4. **Bezpieczeństwo**: W jaki sposób dane są przesyłane z urządzenia do chmury? Czy połączenie pomiędzy urządzeniem a serwerem chmury jest szyfrowane? Jak przechowywane są dane w chmurze? Czy są szyfrowane, a jeśli tak to kto może je odszyfrować? Podczas migracji danych należy pamiętać, że bezpieczeństwo jest wspólnym obowiązkiem użytkownika i dostawcy.
5. **Kompatybilność**: Czy dostawca usług obsługuje wszystkie urządzenia i systemy operacyjne, z których korzystasz lub zamierzasz korzystać?
6. **Warunki korzystania z usługi**: Poświęć chwilę na zapoznanie się z regulaminem korzystania z serwisu. Sprawdź zgodnie z prawem jakiego kraju działa dostawca usługi? Zwróć szczególną uwagę na prawa, które przeniesiesz na swojego usługodawcę podczas korzystania z jego produktu.

Bezpieczeństwo danych

Po wybraniu firmy, której powierzysz przechowywanie danych w chmurze, następnym krokiem jest upewnienie się, że prawidłowo z jej korzystasz. To w jaki sposób uzyskuje się dostęp do danych oraz sposób ich udostępniania, może mieć o wiele większy wpływ na ich bezpieczeństwo niż cokolwiek innego. Kluczowe kroki, które powinieneś podjąć w celu ochrony swoich danych:

1. **Uwierzytelnienie**: Używaj silnych i unikalnych haseł do ochrony danych w chmurze. Jeśli dostawca usługi oferuje opcję uwierzytelnienia dwuskładnikowego, zdecydowanie zalecamy jej włączenie.
2. **Udostępnianie plików i folderów**: Usługi w chmurze sprawiają, że wymiana danych stała się bardzo prosta, czasami nawet zbyt prosta. Niekiedy bardzo łatwo jest przypadkowo udostępnić publicznie swoje dane. Aby temu zapobiec, dobrym pomysłem jest udostępnienie plików tylko określonym osobom lub grupie osób. Jeśli taka osoba nie będzie potrzebowała już dostępu do plików, zwyczajnie ją usuń. Dostawca usług chmurowych powinien również zapewnić łatwy sposób na monitorowanie kto ma dostęp do Twoich plików i folderów.
3. **Ustawienia**: Poświęć chwilę aby dobrze zrozumieć ustawienia zabezpieczeń oferowanych przez operatora chmury. Na przykład, sprawdź czy jeśli przyznasz komuś uprawnienia do pliku, folderu, może on z kolei udostępnić te dane osobom trzecim bez Twojej wiedzy?
4. **Przedłużenie umowy**: Nie zapomnij odnowić subskrypcji/umowy z dostawcą chmury, gdyż możesz mieć problem z dostęp do swoich danych w przypadku wygaśnięcia usługi.

Redaktor gościnny

Tameika Reed (@womeninlinux), założycielka portalu Women in Linux. Prowadzi inicjatywy skupiające się na rozwijaniu kariery w zakresie infrastruktury, cyberbezpieczeństwa, DevSecOps. Prowadzi cotygodniowe spotkania poświęcone tematyce infrastruktury Blockchain. Występowała na OSCon, LISA, Seagl i HashiConf EU.

Źródła

Ataki socjotechniczne:
https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt0992c890a67c09cb/6048ff141322a9094ddefe07/OUCH!_Nov_2020_-_Social_Engineering_v.3-Polish.pdf
Tworzenie haseł w prostszy sposób:
https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt930f1330c1e68833/6047b33bc7198e3af48f8617/201904-OUCH-April-Polish.pdf
Menedżer haseł:
https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltee798afb2a08b806/604a692cacf0d53d70c5e0a6/202004-OUCH-Polish.pdf
Moc aktualizacji:
https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt56ff892c72cf5af8/604a8bae3c41f30bce484fda/OUCH!-May-2020_v3-Polish.pdf

Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz