УДК 004.75

С.А. Лупенко, докт. техн. наук, проф., Ю.Є. Пласконіс
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ОЦІНКА ІСНУЮЧИХ РИЗИКІВ ХМАРНИХ СЕРВІСІВ

S.A. Lupenko, Dr., Prof., Y.Y. Plaskonis

ESTIMATION OF THE RISKS OF CLOUD SERVICES

Час, коли користувачі зберігають усі документи, фотографії і музику на комп'ютері і жорсткому диску поступово добігає кінця. Сьогодні хмарні сховища допомагають вирішити завдання збільшення місця для зберігання усієї не лише персональної, але і корпоративної цифрової власності. Однак, однією з основних невирішених проблем хмарних сервісів є питання безпеки.

Слід зазначити, що інформаційні активи не обмежуються інформацією або даними. Програми і процеси можуть легко виявитися такими ж життєво важливими, як сама інформація. У багатьох сферах, наприклад таких як аналітика і фінанси, використовувані алгоритми і програми часто є власністю і строго секретними для організації. Їх розкриття може спричинити катастрофічні втрати для організації.

Слід зазначити наступні важливі моменти безпеки при використанні хмарних сервісів:

- Паролі можуть бути зламані. Це не означає, що паролі не є безпечними, це означає, що вони уразливі до атак, наприклад dictionary або brute force attacks.
- Дані можуть бути захоплені в дорозі (en route). Для уникнення цього більшість сервісів зберігання шифрують дані, поки вони передаються туди і назад, що робить неможливим їх читання, навіть якщо хтось захоплює файл. Наприклад, якщо хмарне сховище працює через веб-додаток, то використовується протокол HTTPS замість HTTP.
- Однією з найбільших загроз безпеки є соціальна інженерія: створення довіри між хакером і кінцевим користувачем, що примушує кінцевого користувача з радістю передати особисту інформацію. Наприклад, зловмисник може видавати себе за фахівця технічної підтримки.
- Хакери з метою отримання максимальної кількості інформації зазвичай атакують саме сервери хмарного сервісу зберігання, а не його окремих користувачів.
- Дані не завжди недоступні для пошуку і захоплення місцевими органами влади. У США, наприклад, від будь-якої компанії хмарного зберігання можуть зажадати відкрити дані своїх клієнтів для державної перевірки.

Розуміння того, який рівень ризику є допустимим, залежить від оцінки вимог конкретної особи або організації до безпеки і наскільки цінні інформаційні активи - дані, програми і процеси. Після оцінки допустимого ризику можна приймати обґрунтоване рішення про те, які моделі розгортання і моделі надання послуг відповідають потребам і допустимому ризику.

Для вирішення питання безпеки використання хмарних сервісів пропонується цілісна структура безпеки забезпечення зберігання даних в публічній хмарі без демонстрації змісту даних постачальниками послуг хмари, тобто заснована на використанні шифрування даних.

Література

1. Dou El Kefel Mansouri, Mohamed Benyettou, “Risk management in cloud computing”, Third International Conference on Innovative Computing Technology INTECH, London, August 29-31, 2013, IEEE 2013 in way of publishing.