УДК 004.056.53 : 371.315.7

С. В. Коломієць

АНАЛІЗ СУЧАСНИХ МЕТОДІВ АУТЕНТИФІКАЦІЇ У ХМАРНИХ ВЕБ-ПЛАТФОРМАХ

Вінницький національний технічний університет

Анотація

В доповіді розглянуто сучасні методи та особливості аутентифікації для хмарних веб-платформ. Показано, що застосування парольного захисту і одноразових паролів виправдано для приватної веб-платформи, але не забезпечить вимог інформаційної безпеки та поточного законодавства для публічної веб-платформи. Для організації безпечного доступу до хмарних сервісів рекомендується застосовувати технології взаємної аутентифікації на основі застосування механізму кваліфікованого електронного підпису у сертифікатах.

Ключові слова: аутентифікація, веб-платформа, сертифікати, вразливість, пароль.

Abstract

The report deals with modern methods and authentication features for cloud web platforms. It is shown that the use of password protection and one-time passwords for private justified web platform, but do not provide information security requirements and current legislation for public web platform. For the organization secure access to cloud services technologies recommended mutual authentication mechanism on the basis of a qualified electronic signature in the certificate.

Keywords: authentication, web platform, certificates, susceptibility, password.

Вступ

Управління доступом користувачів до хмарним ресурсів являє собою одну з основних проблем для безпечного використання хмарних додатків в корпоративному оточенні. З поширенням численних сервісних концепцій SaaS, PaaS і IaaS управління політиками доступу, в тому числі організація суворої аутентифікації для кожної програми створює певне навантаження на IT-підрозділи підприємств. Користувачам доводиться тримати в пам'яті численні логіни і паролі, що неминуче призводить до втрати паролів, зниження продуктивності і дратує користувачів. До 20% всіх звернень до служби підтримки пов'язано з відновленням втрачених або забутих паролів.

Більш того, IT-підрозділи часто не володіють інформацією про те, з якими саме програмами працюють конкретні користувачі, і як часто здійснюється доступ до цих програм, що фактично призводить до формування тіньових IT і знижує ефективність управління ресурсами. З точки зору контролю доступу виникає також наступне питання: яким чином ви можете гарантувати, що в разі звільнення працівника з компанії він перестане користуватися корпоративними додатками? Нарешті, навіть незважаючи на наявність можливості убезпечити доступ до хмарним ресурсів засобами багатофакторної аутентифікації, IT-підрозділи часто не мають інформації, хто із співробітників все ж подбав про використання такої аутентифікації. В результаті підвищується ймовірність компрометації даних, загроза фішингу, перебору паролів, злому хмарних баз даних і інших погроз.

Метою доповіді є подання сучасних методів застосування різних способів аутентифікації для хмарних веб-платформ, включаючи аутентифікацію за паролем, за сертифікатами, за одноразовими паролями, по ключам доступу і по токену.

Результати дослідження

В доповіді висвітлено такі питання.

1. Проведено аналіз існуючих на сьогодні методів аутентифікації у хмарних веб-платформах [1-2]. При цьому особливу увагу приділено аналізу методів, які є більш стійкими до хакерських атак, а саме для забезпечення більш високої надійності систем безпеки, часто вдаються до таких засобів, як токени і сертифікати.

2. Проведено дослідження впровадження аутентифікації віддалених користувачів за принципом «щось я знаю + щось у мене є», що дозволяє зробити атаку, спрямовану на перехоплення або підбір паролів, безглуздою і значно знизити загрози інформаційної безпеки від отримання зловмисником пароля користувача [3].

3. Проведено аналіз розповсюджених вразливостей і помилок реалізації методів аутентифікації. Проведений аналіз вразливостей показав, що переважна більшість веб-платформ використовують вразливу функцію відновлення пароля, яку можна використовувати для отримання несанкціонованого доступу до інших облікових записів [4].

4. Запропоновано метод аутентифікації за сертифікатами. Використання сертифікатів для аутентифікації – куди більш надійний спосіб, ніж аутентифікація за допомогою паролів. Це досягається створенням в процесі аутентифікації цифрового підпису, наявність якого доводить факт застосування закритого ключа в конкретній ситуації (безвідмовності). Однак труднощі з поширенням і підтримкою сертифікатів робить такий спосіб аутентифікації малодоступним в широких колах [5-6].

Висновки

Проведено аналіз існуючих на сьогодні методів аутентифікації у хмарних веб-платформах та особливу увагу приділено аналізу методів які є стійкі до хакерських атак. Проведено дослідження впровадження аутентифікації віддалених користувачів за принципом «щось я знаю + щось у мене є», на основі якого виявлено, що даний метод є надійним інструментом захисту. Проведено аналіз розповсюджених вразливостей і помилок реалізації методів аутентифікації та виявлено вразливості, які часто зустрічаються у веб-платформах. Запропоновано метод аутентифікації за сертифікатами.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Афанасьєв А. А., Веденєв Л. Т., Воронцов А. А. Аутентифікація. Теорія і практика забезпечення безпечного доступу до інформаційних ресурсів / А.А. Афанасьєв, Л.Т. Веденєв, А.А. Воронцов // Навчальний посібник для вузів. – 2009. – №1. – 552 с.
2. Сабанов А. Г. Основні процеси аутентифікації / А.Г. Сабанов // Проблеми інформаційної безпеки. Комп'ютерні системи. – № 2. – 2012. – С. 102–113.
3. Карпінець В. В., Яремчук Ю. Є. Забезпечення захисту векторних зображень від атак спрямованих на видалення цифрових водяних знаків / В.В. Карпінець, Ю.Є. Яремчук // Вісник Східноукраїнського національного університету імені Володимира Даля. – №15 (204), Частина 1, 2013. – С. 62–68.
4. Сарбуков А. Аутентификация в компьютерных системах / А. Сарбуков, А. Грушо // Системы безопасности. – 2003. – № 5 (53). – С. 25–29.
5. Сабанов А. Г. Аутентифікація при електронному обміні документами А.Г. Сабанов // Доповіді Томського державного університету систем управління і радіоелектроніки. – № 2(24), – 2011. – С. 263–266.
6. Шрамко В. Н. Защита компьютеров: электронные системы идентификации и аутентификации / В. Н. Шрамко // PC Week/RE. – 2004. – № 12. – С. 15–21.

Коломієць Сергій Васильович – студент групи 1УБ-13, факультет менеджменту та інформаційної безпеки, кафедра менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: serhii.kolomiiets@vntu.net.

Науковий керівник: **Василь Васильович Карпінець** – к.т.н., доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця.

Sergey V Kolomiets – student of group 1UB-13, Department of Management and Information Systems Security, Vinnytsia National Technical University, Vinnytsia, email: serhii.kolomiiets@vntu.net.

Supervisor: **Vasyl V Karpinets** – Cand. Sci. (Eng.), Docent of Department of Management and Information Systems Protection, Vinnytsia National Technical University, Vinnytsia.