УДК 004.056

Одинець Т. А.,
Остапченко К. Б.

ЗАГРОЗИ БЕЗПЕКИ В ХМАРНИХ СИСТЕМАХ ТА ШЛЯХИ ЇХ УНИКНЕННЯ

У роботі розглядається проблема загроз безпеки даних, якими оперують додатки та сервіси, що працюють в хмарних системах, а також даних, які безпосередньо зберігаються в хмарних сховищах даних. Виділяються основні види загроз та наводяться рекомендації щодо їх мінімізації.

Ключові слова: хмарні системи, компрометація даних, IT-інфраструктура, кібератака.

Бібл.: 3.

The article deals with the problem of data security threats that is managed by applications and services running on cloud systems, as well as data that is directly stored in cloud storage repositories. In the scope of this article the main types of threats and recommendations for their minimization are described.

Key words: cloud systems, data compromise, IT-infrastructure, cyberattack.

Bibl.: 3.

Актуальність теми дослідження. З огляду на те, як хмарні системи з кожним днем стають все більш поширеними і все більше людей користуються такими сервісами як Google Drive, Dropbox, Amazon Drive, Microsoft OneDrive, постає питання безпеки їх використання. Адже з кожним днем з'являється все більше інформації про прецеденти крадіжки персональних даних та файлів, що зберігались в хмарних системах, одним з яких є атака на акаунт Tesla в хмарі Amazon Web Services. Такі випадки змушують сумніватися в безпеці використання хмарних систем.

Постановка проблеми. Хмарні провайдери, серед яких є такі світові IT-гіганти як Google, Microsoft, Amazon, створюють свої системи дуже доступними як для звичайного користувача, так і для транснаціональної корпорації. А величезна кількість даних, які розміщуються в хмарних системах, робить їх привабливою цілю для хакерів. У цій роботі розглядаються п'ять найбільш поширених загроз безпеки, з якими кінцевий користувач може зіткнутися при зберіганні даних на хмарі, або ж хостингу на ній програмних додатків.

Аналіз останніх досліджень і публікацій. В зв'язку з ростом кількості випадків втрати даних в хмарних системах, з'являється все більше досліджень в цій області та наукових публікацій. Зокрема, провідну роль у таких дослідженнях приймає Cloud Security Alliance (CSA) – некомерційна організація, що займається просуванням найкращих практичних засобів та рекомендацій в розробці систем безпеки на всіх рівнях IT-інфраструктури.

Виділення недосліджених частин загальної проблеми. Дана робота присвячена вивченню та аналізу найбільш поширених загроз безпеки в хмарних системах. Дослідження сфокусовано на вивченні загроз та способів їх уникнення.

Постановка завдання.Визначити найбільш розповсюджені види загроз безпеки в хмарних системах та сформулюватирекомендації щодо захисту в них даних.

Викладення основного матеріалу. Розглянемо п’ять найбільш розповсюджених загроз безпеки в хмарах та наведемо методи їх усунення.

Загроза № 1: Вразливість API хмарних сервісів.

Більшість хмарних сервісів і додатків використовують API для взаємодії з іншими хмарними службами. В результаті безпека API-інтерфейсів безпосередньо впливає на безпеку хмарних сервісів. Більш того, можливість злому збільшується, коли компанії надають стороннім користувачам доступ до API.

На сьогоднішній день вже стали стандартами технології для безпечної передачі даних, такі як OAuth, OpenID Connect, SAML та інші. Розробники фреймворків активно впроваджують ці стандарти в свої продукти, усуваючи необхідність для розробників API самим налаштовувати свої системи на відповідність цим стандартам. Проте, незважаючи на це, досі кожен з розроблених API можуть бути вузьким місцем в питаннях доступності, конфіденційності, цілісності та безпеки. У гіршому випадку це може привести до того, що бізнес втратить конфіденційну інформацію, пов'язану з їх клієнтами і іншими сторонами.

Згідно CSA, кращий спосіб захистити себе від такої загрози - це впровадження додатків і систем моделювання загроз в життєвий цикл розробки. Також CSA рекомендує організувати контроль доступу, використовувати інструменти захисту і раннього виявлення загроз [1].

Загроза №2: Атаки на відмову в обслуговуванні (DDoS).

Атаки DDoS загрожують комп'ютерним мережам вже досить тривалий період часу, однак хмарні технології зробили їх більш поширеними. Ці атаки стимулюють велику потужність обробки і впливають на доступність, продуктивність і швидкодію хмарних систем. Найгірше те, що під час такої атаки неможливо нічого зробити для її усунення. Тому, як тільки це станеться, нічого не залишається робити, за винятком того, щоб сидіти і чекати. Звичайно, також доведеться заплатити за додаткове навантаження, викликану атакою, яка, в залежності від рівня серйозності, може призвести до значних фінансових втрат [2].

Більшість сучасних хмарних сервісів мають системи захисту від DDoS-атак, проте вони не дають абсолютної гарантії. Тому, кращим способом запобігти такій атаці є проведення регулярних перевірок безпеки для виявлення вразливостей до DDoS-атак, а також налаштування ефективної системи обміну критичними ресурсами з адміністраторами для своєчасного сповіщення про загрозу.

Загроза №3: Компрометація облікових записів і обхід аутентифікації.

Така загроза обумовлюється ненадійністю паролів з боку користувачів, або ненадійністю системи аутентифікації з боку провайдера хмарного сервісу. Друга причина є більш серйозною проблемою, адже якщо управління ключами шифрування і сертифікатами відбувається неналежним чином, то під загрозу витоку персональних даних та конфіденційної інформації потрапляють всі користувачі сервісу. Крім того, на корпоративному рівні організації нерідко стикаються з проблемами управління правами та дозволами, коли кінцевим користувачам призначаються значно більші повноваження, ніж в дійсності необхідно. Проблема зустрічається і тоді, коли користувач переходить на іншу посаду в рамках компанії або звільняється. Як правило, мало хто поспішає актуалізувати права на доступ згідно з новими ролями користувача. В результаті виникає неконтрольоване вузьке місце в безпеці.

Відомо, що найбільш збитковим витоком даних за останні 5 років стала атака з метою викрадення ідентифікаційних даних клієнтів Anthem Insurance. Атаку оцінили в 10 балів за Індексом критичності, де було скомпрометовано понад 80 мільйонів облікових записів.

Щодо загрози компрометації даних, CSA рекомендує використовувати:

- механізми багатофакторної аутентифікації;
- одноразові паролі;
- токени;
- смарт-карти;
- USB-ключі.

Це дозволить захистити хмарні сервіси, оскільки застосування вище наведених методів ускладнює процес компрометації паролів.

Загроза №4: Цільові кібератаки.

На сьогоднішній день хмарні системи є досить стійкими до такого роду атак, адже за даними досліджень Cisco, кіберзлочинці ще не володіють достатнім набором інструментів для обходу сучасних систем шифрування, які використовуються провайдерами, або ж для їх обходу потрібні колосальні ресурси. Тим не менш, загроза цільової кібератаки не виключена навіть для найбільш сучасних систем, серед яких найбільш вразливими є хмарні SaaS-сервіси (Software as a Service), де користувач не контролює нічого, окрім власних даних. Більш безпечними є IaaS-сервіси (Infrastructure as a Service), де користувач має можливість самостійно слідкувати за рівнем безпеки даних та встановлювати засоби їх захисту.

Варто зазначити, що у випадку, якщо зловмиснику вдалось закріпити власну присутність в цільовій інфраструктурі, його виявлення стає доволі серйозним та важким завданням.

CSA рекомендує проводити спеціалізоване навчання співробітників по розпізнаванню методів зловмисника, використовувати розширені інструменти безпеки, вміти правильно управляти процесами, знати про планові відповідні дії на інциденти, застосовувати профілактичні методи, що підвищують рівень безпеки інфраструктури [1].

Загроза №5: Ризики, пов’язані зі зловживанням хмарними сервісами.

Хмари можуть використовуватися легітимними і нелегітимними організаціями. Мета останніх - використовувати хмарні ресурси для здійснення зловмисних дій: запуску DDoS-атак, відправки спаму, поширення шкідливого контенту та інше. Постачальникам послуг вкрай важливо вміти розпізнавати таких учасників, для чого рекомендується детально вивчати трафік і використовувати інструменти моніторингу хмарних середовищ.

Ще однією причиною для таких загроз є повна міграція даних корпоративної системи до хмарних сервісів. Часто організації ігнорують ризики, які можуть бути завдані через вразливості хмарних систем, не створюючи власних систем резервування. Як результат, виникає недотримання концепції сегментування мережі, що може призвести до повної втрати даних при першій же помилці роботи хмарної системи або атаці на неї [3].

CSA рекомендує використовувати стратегію «безпеки в глибину», впроваджувати механізми багатофакторної аутентифікації, системи виявлення вторгне-

нь, дотримуватися концепції сегментування мережі і принципу надання найменших привілеїв.

Висновки. Сучасні хмарні системи є новим етапом розвитку IT-інфраструктури і вже сьогодні поступово витісняють з ринку старші покоління систем зберігання даних та хостингу додатків за рахунок надання користувачам миттєвого доступу до широкого спектру ресурсів і додатків. Проте, важливо пам'ятати, що всі хмарні провайдери мають вразливі місця та несуть потенційні загрози користувачам. Однак, ці загрози можна мінімізувати, дотримуючись вище наведених рекомендацій.

Список використаних джерел

1. Wei J. Cloud Security Alliance. Security as a Service [Електронний ресурс] / електрон. наук. вид. Security Guidance for Critical Areas of Focus in Cloud. – 2015. – № 4. – С.102–144. – Режим доступу до журн. : https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf.

2. Ali M. Security in cloud computing: Opportunities and challenges [Електронний ресурс] : електронневидання Elsevier / Khan S. U., Vasilakos A. V. // An International Journal. – 2017. – № 305. – С. 359–373. – Режимдоступудожурн. : https://pdfs.semanticscholar.org/40e7/adc40b609cd13f9b84a5cc9ae780ffba6ec0.pdf.

3. Zissis D. Addressing cloud computing security issues [Електронний ресурс] / Lekkas D. // Future Generation Computer Systems. – 2012. – № 28. – С.15–43. – Режим доступу до журн. : https://doi.org/10.1016/j.future.2010.12.006.

ДОВІДКА ПРО АВТОРІВ

Остапченко Костянтин Борисович – к.т.н., доцент, кафедра технічної кібернетики, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського».

Ostapchenko Konstantin – doctor of technical sciences, associate professor, Department of Tehnical Cybernetics, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”.

E-mail: okb2003@ukr.net

Одинець Тетяна Анатоліївна – студентка, кафедра технічної кібернетики, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського».

Odynets Tetiana – student, Department of Tehnical Cybernetics, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”.

E-mail: todynets@gmail.com

Odynets Tetiana,
Ostapchenko Konstantin

SECURITY THREATS IN CLOUD SYSTEMS AND WAYS OF THEIR DESTRUCTION

Relevance of research topic. Considering how cloud systems become more common every day, the data security issues that is stored on them become more actual. More and more people use services such as Google Drive, Dropbox, Amazon Drive, Microsoft OneDrive and others to save and access their files in an easy way. However, more and more information about the precedents of theft of personal data and files stored in cloud-based systems appears every day, one of which is the attack on the Tesla account in the Amazon Web Services cloud. Such cases make it doubt the safety of cloud systems.

Formulation of the problem. Cloud providers, among which there are such global IT giants as Google, Microsoft and Amazon, create their systems very affordable for both the ordinary user and the multinational corporation. And the huge amount of data stored in cloud systems makes them an attractive target for hackers. This article discusses the five most common security threats that an end-user may face when storing data on a cloud, or host software applications on it.

Analysis of recent research and publications. Due to the growing number of cases of data loss in cloud systems, more research in this area and scientific publications are emerging. In particular, the Cloud Security Alliance (CSA), a nonprofit organization dedicated to promoting best practices in developing security systems at all levels of the IT infrastructure, takes on the leading role in such research.

Selection of unexplored parts of the general problem. This article is devoted to the study and analysis of the most common security threats in cloud systems. The research focuses on the study of threats and ways to avoid them.

Setting objectives. Identify the most common types of threats and describe how to protect your data.

Presentation of the main material. The analysis and definition of the 5 most common security threats in the clouds were conducted, as well as methods and tools for their elimination.

Conclusions. Modern cloud systems are a new stage in the development of IT infrastructure and are now gradually replacing older generations of storage and hosting systems from the market by providing users with instant access to a wide range of resources and applications. But it's important to remember that all cloud providers have vulnerabilities and potential threats to users. However, these threats can be minimized by following the above recommendations.

Key words: cloud systems, data compromise, IT-infrastructure, cyberattack.