УДК 004.56

Г.В. Шимчук, О.С. Голотенко, к.т.н., доцент, Р.З. Золотий, к.т.н., доцент
Тернопільський державний технічний університет імені Івана Пулюя

ПРОБЛЕМИ БЕЗПЕКИ ХМАРНИХ СЕРЕДОВИЩ

G.V. Shymchuk, O.S. Holotenko. Ph. D., Assoc. Prof., R.Z. Zoloty, Ph. D., Assoc. Prof.

SECURITY PROBLEMS OF CLOUD ENVIRONMENTS

Сучасний бізнес хоче всього: безпечні дані та програми, доступні будь-де з будь-якого пристрою. Це можливо завдяки хмарним середовищам, але є невід'ємні проблеми безпеки хмарних обчислень, щоб втілити це в реальність.

Хмарні середовища дозволяють легко обмінюватися даними, що зберігаються в них. Ці середовища доступні безпосередньо з загальнодоступного Інтернету та включають можливість легко обмінюватися даними з іншими сторонами через прямі запрошення електронною поштою або шляхом спільного використання загальнодоступного посилання на дані.

Простота обміну даними в хмарі – хоча це головний актив і ключ до співпраці в хмарі – викликає серйозні занепокоєння щодо втрати або витоку даних. Насправді 69% організацій вказують на це як на найбільшу проблему безпеки хмарних технологій. Обмін даними за допомогою загальнодоступних посилань або налаштування хмарного сховища на загальнодоступне робить їх доступними для будь-кого, хто знає про посилання, і існують спеціальні інструменти для пошуку в Інтернеті цих незахищених хмарних розгортань.

Конфіденційність і конфіденційність даних є основною проблемою для багатьох організацій. Положення про захист даних, як-от Загальний регламент ЄС щодо захисту даних (GDPR), Закон про мобільність і доступність медичного страхування (HIPAA), Стандарт безпеки даних індустрії платіжних карток (PCI DSS) та багато інших зобов'язують захистити дані клієнтів і накладають суворі штрафи за збої безпеки. Крім того, організації мають велику кількість внутрішніх даних, необхідних для збереження конкурентної переваги.

Розміщення цих даних у хмарі має свої переваги, але також створює серйозні проблеми з безпекою для 66% організацій. Багато організацій запровадили хмарні обчислення, але їм не вистачає знань, щоб переконатися, що вони та їхні співробітники використовують їх безпечно. У результаті конфіденційні дані знаходяться під загрозою розголошення, про що свідчить величезна кількість порушень хмарних даних.

Фішери зазвичай використовують хмарні програми та середовища як привід для своїх фішингових атак. Зі зростанням використання хмарної електронної пошти (G-Suite, Microsoft 365 тощо) і служб обміну документами (Google Drive, Dropbox, OneDrive) співробітники звикли отримувати електронні листи з посиланнями, які можуть попросити їх підтвердити обліковий запис. облікові дані, перш ніж отримати доступ до певного документа або веб-сайту.

Це дозволяє кіберзлочинцям легко дізнатися облікові дані співробітника для хмарних сервісів. У результаті випадкове відкриття хмарних облікових даних викликає серйозне занепокоєння для 44% організацій, оскільки це потенційно ставить під загрозу конфіденційність і безпеку їхніх хмарних даних та інших ресурсів.

Багато організацій мають стратегії реагування на внутрішні інциденти кібербезпеки. Оскільки організація володіє всією внутрішньою мережевою інфраструктурою, а персонал служби безпеки працює на місці, можна заблокувати інцидент. Крім того, це право власності на їх інфраструктуру означає, що компанія, ймовірно, має видимість, необхідну для визначення масштабу інциденту та виконання відповідних дій з усунення.

Завдяки хмарній інфраструктурі компанія має лише часткову видимість і право власності на свою інфраструктуру, що робить традиційні процеси та інструменти безпеки неефективними. У результаті 44% компаній стурбовані своєю здатністю ефективно реагувати на інциденти в хмарі.

Правила захисту даних, такі як PCI DSS і HIPAA, вимагають від організацій продемонструвати, що вони обмежують доступ до захищеної інформації (даних кредитних карток, медичних записів пацієнтів тощо). Це може вимагати створення фізично або логічно ізольованої частини мережі організації, яка буде доступна лише для працівників, які мають законну потребу в доступі до цих даних.

Під час переміщення даних, захищених цими та подібними правилами, у хмару досягти та продемонструвати відповідність нормативним вимогам може бути складніше. Завдяки хмарному розгортанню організації мають можливість переглядати та контролювати лише деякі рівні своєї інфраструктури. Як наслідок, 42% організацій вважають відповідність законодавству та нормативним вимогам основною проблемою безпеки хмари та потребують спеціалізованих рішень відповідності хмарі.

Більшість хмарних провайдерів мають кілька територіально розподілених центрів обробки даних. Це допомагає підвищити доступність і продуктивність хмарних ресурсів і полегшує для постачальників послуг гарантування того, що вони здатні підтримувати угоди про рівень обслуговування в умовах руйнівних подій, таких як стихійні лиха, відключення електроенергії тощо.

Організації, які зберігають свої дані в хмарі, часто не знають, де насправді зберігаються їхні дані в масиві центрів обробки даних CSP. Це викликає серйозні занепокоєння щодо суверенітету даних, місця розміщення та контролю для 37% організацій. З нормативними актами щодо захисту даних, такими як GDPR, які обмежують, куди можна надсилати дані громадян ЄС, використання хмарної платформи з центрами обробки даних за межами затверджених зон може привести організацію до стану невідповідності нормативним вимогам. Крім того, різні юрисдикції мають різні закони щодо доступу до даних для правоохоронних органів і національної безпеки, що може вплинути на конфіденційність даних і безпеку клієнтів організації.

Хмара надає організаціям ряд переваг; однак вона також має свої власні загрози безпеці та проблеми. Хмарна інфраструктура дуже відрізняється від локального центру обробки даних, і традиційні інструменти та стратегії безпеки не завжди здатні ефективно захистити її.

Література

1. A. Alshammari, S. Alhaidari, A. Alharbi and M. Zohdy, "Security Threats and Challenges in Cloud Computing," 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), 2017, pp. 46-51, doi: 10.1109/CSCloud.2017.59.

2. Pavan Muraidhara, "Security issues in cloud computing and its countermeasures", International Journal of Scientific & Engineering Research, vol. 4, no. 10, October 2013.

3. M. Zeller, R. Grossman, C. Lingenfelder, M. Berthold, E. Marcade, R. Pechter, et al., "Open standards and cloud computing: KDD-2009 panel report" in , Paris, France:KDD, pp. 11-18, 2009.

4. Tabrizchi, H., Kuchaki Rafsanjani, M. A survey on security challenges in cloud computing: issues, threats, and solutions. J Supercomput 76, 9493–9532 (2020). https://doi.org/10.1007/s11227-020-03213-1

5. Subramanian N, Jeyaraj A (2018) Recent security challenges in cloud computing. Comput Electr Eng 71:28–42