Львівський державний університет безпеки життєдіяльності

Національний університет Львівська політехніка

Департамент кіберполіції Національна поліція України

Львівська міська рада

LVIV IT CLUSTER

softserve

UnderDefense

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
IV Міжнародної науково-практичної конференції
ІБІТ 2022

30 листопада 2022 року

УДК 004.75

БЕЗПЕКА ІНФОРМАЦІЇ У ХМАРНИХ СХОВИЩАХ

Владислав Горон[1], Орест Полотай[2], Уляна Пановик[2]

[1]Кафедра безпеки інформаційних технологій Національного університету "Львівська політехніка", м. Львів, Україна
[2]Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна

Анотація. *Описано хмарні сховища, типи хмар та способи захисту інформації в марних сховищах.*
Ключові слова: *хмарні сховища, хмарна безпека.*

Abstract. *Describes cloud storage, types of clouds and ways to protect information in useless storage.*
Keywords: *cloud storage, cloud security.*

Хмарне сховище – це модель комп'ютерного сховища даних, у якій цифрові дані зберігаються в логічних пулах, які називаються "хмарою". Фізичне сховище охоплює кілька серверів, а фізичне середовище, як правило, належить і керується хостинговою компанією.

Зазвичай використовуються три типи хмар:

1. Громадські хмари – це хмарні ресурси, такі як обладнання, сховище та мережеві пристрої, належать і керуються стороннім постачальником хмарних послуг і надаються через інтернет.

2. Приватні хмари – використовуються виключно однією організацією та можуть бути фізично розташовані в локальному центрі обробки даних або розміщені стороннім постачальником хмарних послуг.

3. Гібридні хмари – це поєднання приватної хмари з публічною хмарою. У гібридній хмарі дані та програми можуть переміщатися між приватною та загальнодоступною хмарами для більшої гнучкості та додаткових можливостей розгортання.

В наш час людям набагато зручніше користуватися хмарними сховищами. Вони не займають зайве місце, до них легко доступитися в любий момент, потрібен тільки Інтернет. Також компаніям краще використовувати хмари, тому що легше виділити місце у хмарі, а між зберігати дані, наприклад, на флешках або дисках. Тому все більше і більше компаній задумують над тим як покращити безпеку інформації у хмарних сховищах.

Хмарна безпека – це набір політик, технологій, програмного забезпечення та програм, які захищають ваші дані, що зберігаються не на вашому комп'ютері, а в Інтернеті.

Хмарна безпека є дуже важливою, тому що все більше і більше інформації зберігається у хмарі і це дає можливість зловмисникам отримати її, якщо хмара є недостатньо захищеною. Якщо дехто зберігає в хмарі тільки свої сімейні фотографії і відео, щоб вони не займали місце на комп’ютері і втрата таких даних не буде критичною, то компанії зберігають свої документи і важливі дані своїх працівників, втрата цих даних може призвести до великих фінансових втрат.

Так як зараз багато роботи робиться дистанційно, то ризики викрадення інформації з хмари збільшуються. В таких випадках безпека мобільних пристроїв має особливе значення. В компанії може бути прекрасний захист системи, але якщо працівник має можливість зайти в систему зі свого пристрою, то ризик викрадення інформації є дуже великим. Для таких випадків є політика Bring-Your-Own-Device (BYOD. Це політика, згідно з якою співробітникам дозволено або рекомендується використовувати особисті мобільні пристрої (телефони, планшети, ноутбуки) для доступу до корпоративних даних та систем, але вони мусять дотримуватися певних правил для того, щоб зменшити ризик викрадення інформації.

Є декілька способів покращення безпеки хмари:

1. Підключення багатофакторної автентифікації (MFA). З кожним днем зловмисники знаходять все нові і нові способи отримати доступ до вашого аккаунту. Тому зараз комбінації імені користувача та пароля недостатньо. MFA є одним із найдешевших, але найефективніших засобів контролю безпеки, які запобігають доступу потенційних хакерів до ваших хмарних програм.

2. Керувати доступом користувачів, щоб покращити безпеку хмарних обчислень. Більшості співробітників не потрібен доступ до кожної програми, кожної інформації чи кожного файлу у вашій хмарній інфраструктурі. Встановлення відповідних рівнів авторизації гарантує, що кожен співробітник може переглядати або маніпулювати лише тими програмами чи даними, які необхідні йому для виконання роботи.

3. Відстежування дій кінцевих користувачів за допомогою автоматизованих рішень для виявлення зловмисників. Моніторинг у режимі реального часу та аналіз дій кінцевих користувачів можуть допомогти вам виявити порушення, які відрізняються від звичайних шаблонів використання, наприклад, вхід із раніше невідомої IP-адреси або пристроїв.

4. Створення комплексного процесу виходу працівника з системи. Коли співробітники залишають вашу компанію, переконайтеся, що вони більше не мають доступу до вашого хмарного сховища, систем, даних, інформації про клієнтів та інтелектуальної власності.

5. Регулярне проведення навчань співробітників із захисту від фішингу. Хакери можуть отримати доступ до захищеної інформації, викравши облікові дані співробітників за допомогою методів соціальної

інженерії, таких як фішинг, підробка веб-сайтів і шпигунство в соціальних мережах. Пропонувати постійне навчання – найкращий спосіб запобігти тому, щоб співробітники стали жертвами цих шахраїв і скомпрометували конфіденційні дані вашої компанії.

Як підсумок можна сказати, що хмарне середовище є дуже зручним і на сьогоднішній день захищеним, але немає гарантії, що ваші дані захищені на всі сто відсотків, тому що хакери кожен раз придумують щось нове для того, щоб отримати персональну інформацію працівників. Також кожен працівник мусить дотримуватися певних правил для того, щоб зменшити ризики витоку даних. Компанія може мати дуже хороший захист, але якщо їх працівники не дотримуються правил безпеки, то хакери зможуть обійти любий захист.

Інформаційні джерела

1. Стаття “Cloud storage” на сторінці вікіпедії – https://en.wikipedia.org/wiki/Cloud_storage.

2. Belej O., Nestor N., Panchak S., Polotai O.I. Developing a Model of Cloud Computing Protection System for the Internet of Things. 2020 IEEE 16th International Conference on the Perspective Technologies and Methods in MEMS Design, MEMSTECH 2020 – Proceedings, 2020, pp. 53–58.

УДК 514.18:004.056

ЗБЕРЕЖЕННЯ КРЕСЛЕНИКІВ У ВЕКТОРНІЙ ГРАФІЦІ

Олена Гумен, Ірина Селіна, Артем Василенко

Національний технічний університет України
Київський політехнічний інститут імені Ігоря Сікорського, Київ, Україна

Анотація. *Необхідність забезпечення збереження інформації, зокрема креслеників та інших документів, є наразі дуже актуальною. Все ширше застосування набувають для цього хмарні сховища. Головною перевагою векторної графіки є можливість зміни розмірів зображення без втрати якості картинки, що значно спрощує роботу з графікою і підвищує якість кінцевого результату.*

Ключові слова: *векторна графіка, хмарні документи, кресленики.*

Abstract. *The need to ensure the preservation of information, in particular blueprints and other documents, is currently very urgent. Cloud storage is increasingly used for this purpose. The main advantage of vector graphics is the ability to change the size of the image without losing image quality, which greatly simplifies work with graphics and improves the quality of the final result.*

Keywords: *vector graphics, cloud documents, drawings.*