МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеський національний технологічний університет
Університет Інформатики і прикладних знань, м.Лодзь, Польща
Національний технічний університет України «Київський політехнічний інститут»
Навчально-науковий інститут комп'ютерних систем і технологій «Індустрія 4.0» ім. П.М. Платонова

XXIII Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Матеріали конференції

Одеса

20-21 квітня 2023 р.

Стан, досягнення та перспективи інформаційних систем і технологій / Матеріали XXIII Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 20-21 квітня 2023 р**.** - Одеса, Видавництво ОНТУ, 2023 р. – 449 с.

Збірник включає матеріали доповідей учасників конференції, які об'єднані за тематичними напрямками конференції.

Збірник буде корисним як для фахівців і працівників фірм, зайнятих в області IT, так і для викладачів, магістрів і студентів вищих навчальних закладів, які навчаються за напрямами і спеціальностями програмного забезпечення, обчислювальної техніки і автоматизованих систем, прикладної математики та обробки інформації, буде корисним професіоналам з комп'ютерного моделювання та розробки комп'ютерних ігор.

Результати досліджень у збірнику представляють собою своєрідний зріз сучасного стану справ в перерахованих галузях знань, який може допомогти як фахівцям, так і студентам університетів скласти загальну картину розвитку інформаційних технологій та пов'язаних з ними питань.

Наукові праці згруповані за напрямками роботи конференції та наведені в алфавітному порядку прізвищ авторів.

Матеріали (тези доповідей) друкуються в авторській редакції. Відповідальність за якість та зміст публікацій несе автор.

Матеріали подано українською та англійською мовами.

Редактор збірника Котлик С.В.

УДК 004.056

МЕТОДИ ЗАХИСТУ ХМАРНИХ СЕРВІСІВ ВІД ВНУТРІШНІХ ЗАГРОЗ ТА ВИТОКІВ ДАНИХ

ДЕМЧУК В. С. (viktoriia.hlahovska.kb.2019@lpnu.ua)
Національний університет «Львівська політехніка»

Запропоновані методи захисту від внутрішніх загроз, які спричинені діями умисними та випадковими діями персоналу, які дозволять знизити ризик витоку та порушення цілісності чи конфіденційності даних.

Актуальність проблеми. Хмарні сервіси масово використовуються в організаціях для вирішення різноманітних задач. Впровадження сервісів дало можливість використовувати потужні ресурси та забезпечувати зберігання даних в безпечному місці з можливістю швидкого доступу. Проте, це стало значним джерелом небезпеки не тільки від зовнішніх зловмисників, а й від внутрішніх. Тому через зростаючу кількість випадків крадіжки даних, які зберігаються на хмарних сервісах, проблема захисту є актуальною.

Хмарні сервіси стали рішенням багатьох задач. Дозволили зберігати великі обсяги даних в безпечних місцях, що знизило ризик втрати даних та сприяло можливості швидкого доступу з будь-якого місця. Завдяки сервісам пришвидшилась обробку великого обсягу даних. Дозволило підприємствам зменшити витрати на обладнання та інфраструктуру. Забрало проблему масштабування.

Зростання популярності хмарних сервісів сприяло розробці систем та методів захисту даних. Більшість постачальників забезпечують надійний захист для свого продукту, проте основні механізми в таких системах захисту спрямовані на захист від зовнішніх загроз. Тому дані, які зберігаються на хмарних сервісах, все частіше стають ціллю для атаки. Внутрішнім зловмисником може бути працівник, у якого є доступ до даних, компанії, яка використовує послуги, а також працівник компанії, яка постачає хмарні послуги.

Однією з можливих загроз є витік даних, який може статись через недбалість персоналу, неправильну конфігурацію системи чи спрямовані зловмисні дії.

Також ще одним варіантом сценарію атаки може бути отримання працівником доступу до сервісу з привілейованого акаунту, який йому не належить, що може призвести до зміни налаштувань, витоку даних, втрати доступу до даних чи порушення цілісності чи конфіденційності даних.

Тобто, основним джерелом загрози є людина, яка отримала невідповідний до її потреби доступ. Отже, методи для захисту хмарних сервісів мають бути спрямовані на обмеження доступу до даних, контроль за діями на сервісі, покращення системи автентифікації.

Методи для вирішення проблеми.

Першим методом для вирішення проблеми є впровадження мікросегментації та концепції «нульової довіри». Мікросегментація – це створення певних зон або кишень для ізоляції робочих навантажень одна від одної, щоб вони могли бути захищені індивідуально. Така процедура тісно пов'язана з підходом "нульової довіри". Ці сегменти мають різні рівні безпеки і кожен із них захищається окремо. Метод дозволяє розгортати гнучкі індивідуальні безпекові політики для кожного сегмента, у тому числі на рівні додатків. Призначення способів захисту кожного окремого сегмента підвищує стійкість до атак.

Основною задачею є контроль доступу та розроблення рольової моделі. Ці методи взаємопов’язані методи необхідні для зменшення ризику витоку даних. Користувачам та адміністратором призначаються мінімально необхідні права доступу до тих підсистем, з якими вони працюють. Реалізація відбувається завдяки встановленню різних рівнів доступу та впровадженні обмежень. Для цього використовується рольова модель, тобто метод, який дозволяє встановити ролі користувачам да визначити ресурси, до яких потрібний доступ. При реалізації даного методу необхідно зменшити ризик помилкової авторизації чи

неправильного визначення рівню доступу та ролі. Важливим аспектом є те, що система залишається вразливою до атак інших типів, тому необхідно забезпечити достатній захист, щоб уникнути несанкціонованого доступу. Також забезпечити достатній контроль над даними, для цього використовуються методи наведені нижче.

Впровадження інструментів для моніторингу дозволить цілодобово отримувати звіти про стан системи з погляду її цілісності, доступності, забезпечення конфіденційності інформації та своєчасне реагування на інциденти, незалежно від їх масштабу.

Важливим кроком є використання багатофакторної автентифікації.

Введення механізму шифрування даних, які зберігаються в хмарному сервісі, є необхідним для забезпечення безпеки даних. Шифрування даних перед збереженням в хмарному сервісі зменшить ризик несанкціонованого доступу внутрішніх зловмисників і від працівників провайдера послуг, які зловживають своїми обов'язками.

Ще одним механізмом для відслідковування є аудит дій персоналу. Система дозволить слідкувати за тим, яким чином працівники використовують дані. Також сприятиме швидкому виявленню недоречного чи забороненого використання даних.

Висновок. Захист хмарних сервісів потрібний не тільки від зовнішніх загроз, а також від внутрішніх зловмисників. Основною проблемою при впроваджені методів захисту даних може стати недостатній рівень кваліфікації відповідальної особи та недостатньо повно розроблена рольова модель. Найкращим захистом від внутрішніх загроз та витоку інформації буде поєднання всіх або хоча б декількох з наведених методів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. S. M. Thampi and B. Bhushan, "Data Security in Cloud Computing," in 2014 International Conference on Contemporary Computing and Informatics (IC3I), Mysore, India, 2014, pp. 433-438, doi: 10.1109/IC3I.2014.7019788.
2. R. L. Krutz and R. D. Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Hoboken, NJ: Wiley, 2010.

УДК 004.6

ІНФОРМАЦІЙНА СИСТЕМА АНАЛІЗУ ВСТУПНИХ ПРОПОЗИЦІЙ НА СПЕЦІАЛЬНОСТІ 122 ТА 123 ПО ОБЛАСТЯМ УКРАЇНИ

ДЕРГАЧОВ М.А., СЕЛІВАНОВА А.В.
(maximadda2001@gmail.com, av_selivanova@ukr.net)
Одеський національний технологічний університет

Метою даної роботи є розробка багатокористувацького WEB-додатку, який дозволить користувачам зручно та ефективно збирати та переглядати дані щодо вступних пропозицій по спеціальностям, областям та університетам України. Додаток буде забезпечувати користувачів зручним та швидким доступом до необхідної інформації. Для розробки додатку використовується мова Python, фреймворк для розробки веб-додатків Django та редактор коду Visual Studio Code, а також система для управління ізольованими Linux-контейнерами Docker.

У наш час зростає потреба в ефективному аналізі вступних пропозицій за різними спеціальностями у заклади вищої освіти (ЗВО) України. Це пов'язано з тим, що кількість заявок на вступ до ЗВО значно перевищує кількість доступних місць, і це робить конкурс на вступ настільки високим, що деякі абітурієнти не можуть отримати бажану спеціальність або взагалі місце у навчальному закладі.