Косиченко О. О.,
доцент кафедри
інформаційних технологій
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

ОСНОВНІ ПРОБЛЕМИ БЕЗПЕКИ ПРИ ВИКОРИСТАННІ ХМАРНИХ ПОСЛУГ ПІДПРИЄМСТВАМИ

Популярність хмарних послуг останніми роками стрімко зростає. Перспективи економії на капітальних та операційних витратах, а також масштабованість та еластичність спонукали компанії переходити на хмарні послуги. Однак перехід на хмарні технології пов'язаний із великою кількістю проблем. Одна з них – безпека, величезна проблема для організацій, які хочуть перейти на хмарні технології.

Дані організації – один із самих коштовних активів. Тому їх безпека відіграє важливу роль для багатьох організацій при переході на хмарні технології. Постачальники хмарних послуг (CSP – cloud service providers) тримають у секреті точне місце розташування своїх центрів обробки даних. Хоча це й передова практика в області фізичної безпеки, багато організацій – потенційні клієнти бояться не знати місцезнаходження зберігання своїх даних і відмовляються від хмарних сервісів.

Інформаційний суверенітет також відіграє велику роль у питанні переходу на хмарні технології. Організації не хочуть втрачати доступу до своїх даних через юридичні складнощі. Дотримання нормативних вимог відповідно Європейського загального регламенту захисту персональних даних (GDPR) – одна з ключових проблем для компаній. Порушення GDPR та інших нормативних актів спричиняє великі фінансові штрафи, чого більшість організацій хочуть уникнути. З цієї причини багато організацій вважають за краще зберігати конфіденційні дані (персональну інформацію тощо) локально.

Вирішальне значення для організації, яка використовує хмарне сховище, грають системи запобігання втрати даних (DLP – Data Leak Prevention). Випадкове видалення даних може статися з боку самої організації. У угоді про рівень послуг (SLA – Service Level Agreement) може бути обговорено про сприяння відновленню систем та інформації з боку CSP. Якщо CSP не зможе виконати SLA, клієнт зазнає великих збитків. Тому організації хочуть бути впевненими у безпеці своїх резервних копій, адже у разі втрати чи пошкодження даних їм потрібно, щоб дані були відновлені в рамках цільового часу відновлення (RTO – Recovery time objective) та цільових точок відновлення (RPO – Recovery Point Objective).

Багато компаній для вирішення своїх завдань використовують програмне забезпечення та послуги від різних постачальників. У зв'язку з цим подібні

організації при переході в хмару іноді змушені прийняти багатохмарну модель. За даними дослідження, проведеного компанією Tripwire у 2021 році, 98% фахівців з безпеки, що працюють у сфері багатохмарних середовищ, вважають таку модель більш ризикованою з точки зору безпеки. Респонденти того ж опитування зазначили, що важко знайти фахівців з безпеки, які є експертами у всіх хмарних середовищах, що використовуються різними CSP.

Підвищені ризики мультихмарної моделі змушують організації відмовлятися від деяких переваг кількох хмарних послуг на користь одного CSP. Вибір одного CSP замість іншого – не завжди просте рішення. Деякі постачальники послуг хмари можуть ускладнити перехід організації до інших постачальників. Перед вибором CSP компанія має ретельно вивчити умови використання хмарних послуг конкретного CSP.

Відсутність належної обачності може сповільнити реагування служб безпеки на кібератаки. Більшість CSP працюють за моделлю спільної відповідальності, коли йдеться про забезпечення безпеки у хмарі, тому клієнтам хмарних сервісів дуже важливо розуміти свою роль і роль CSP у цій моделі. Кібератаки неминучі, тому компаніям необхідно мати плани реагування на різні інциденти та бути впевненими у методах захисту провайдерів.

При оцінці варіанта публічної хмари організація повинна розуміти, що в такій моделі для скорочення витрат використовується розрахована на багато користувачів ліцензія. Клієнти сервісів повинні бути впевнені в CSP та методах «глибокого захисту», адже відсутність багаторівневого захисту дозволить хакеру здійснювати серії кібератак після однієї успішної спроби.

Організації, які використовують критично важливі сервіси у хмарі, можуть серйозно постраждати від DoS та DDoS-атак, що паралізують бізнес-операції. Щоб мінімізувати ризик таких атак, компанії повинні прагнути усунення єдиних точок відмови при виділенні робочих навантажень.

Більшість завдань із забезпечення, керування та моніторингу робочих навантажень у хмарі виконуються через виклики способів взаємодії однієї комп'ютерної програми з іншими (API – Application Programming Interface, інтерфейс прикладного програмування). Тому важливість надійних API не можна недооцінювати, адже від них залежить безпека та доступність спільних хмарних сервісів. Відсутність грамотно налаштованої авторизації, контролю доступу та моніторингу API може призвести до різних порушень та руйнівних атак хакерів.

Можливість стихійного лиха, хоча і не відноситься до атак, все ж таки є подією, що порушує роботу хмарних сервісів. Якщо стихійне лихо зруйнує центри обробки даних CSP, це призведе до серйозних порушень у роботі підприємств, які використовують центри обробки даних, адже навіть, незважаючи на передові методи резервування, у разі стихійного лиха ризик втрати інформації досить високий.

Перехід у хмару – важливе, але ризиковане бізнес-рішення, що вимагає грамотної оцінки всіх «за» і «проти». Помилкове рішення здатне завдати непоправної шкоди організації, але при ретельному дотриманні заходів безпеки та оцінки ризиків можна зробити хмарні послуги чудовим інструментом для розвитку компанії.

Список використаних джерел:

1. Prinzlau M. 6 security risks of enterprises using cloud storage and file sharing apps. URL: https://digitalguardian.com/blog/6-security-risks-enterprises-using-cloud-storage-and-file-sharing-apps.
2. Semeney A. What are the Top Cloud Computing Security Issues for Businesses. URL: https://www.devteam.space/blog/author/alexey-semeney/
3. Dotson C. Practical Cloud Security. USA : O'Reilly Media Inc. 195 p.

Костенко О. В.,
завідувач науково-дослідної лабораторії теорії і права цифрових трансформацій науково-дослідного центру цифрових трансформацій і права Національної академії правових наук України, доктор філософії в галузі права
Прокопович-Ткаченко Д. І.,
в. о. завідувача кафедри кібербезпеки та інформаційних технологій Університету митної справи та фінансів, кандидат технічних наук, доцент

УПРАВЛІННЯ ІДЕНТИФІКАЦІЙНИМИ ДАНИМИ: ІДЕНТИФІКАЦІЯ IoT ЯК БАЗОВИЙ ЕЛЕМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Одним із ключових елементів технологій та систем передачі даних є наявність інформації за якою можливо ідентифікувати суб'єктів та об'єктів за притаманні їм ідентифікаційні атрибути – ідентифікаційними даними.

Ідентифікаційними даними вважається інформація про конкретного суб'єкта в формі одного або декількох атрибутів, що дозволяють суб'єкту бути в достатній мірі відмінним в певному контексті або набір атрибутів особи, які дозволяють цій особі відрізнятися від інших осіб у конкретному контексті, а саме е-екосистемі IoT.

Разом із тим, управлінням ідентифікаційними даними в широкому сенсі прийнято вважати набір прийомів, що дозволяють управляти процесами ідентифікації, автентифікації і авторизації фізичних і юридичних осіб, пристроїв IoT в режимі он-лайн з метою отримання електронних сервісів та даних.

Сучасний IoT являє собою локальні об'єднання автономних мікро електромеханічних систем (MEMS), радіотехнологій передачі даних, програмних продуктів, електронних сервісів, Інтернету та галузевих або соціальних інформаційно-комунікаційних хабів (е-екосистем).