

ПЗ-10. Конфіденційність та безпека хмарних технологій та сервісів на їхній основі

Принцип 1: Створення уніфікованої стратегії керування доступом

- У хмарних обчисленнях традиційний периметр переміщується за межі корпоративного центру обробки даних, тому ідентифікація замінює мережі як основний кордон довіри. З цією метою уніфікована стратегія керування ідентифікацією та доступом є важливою для захисту хмари.
- Щоб досягти цього, ви повинні звернути увагу на:
- Уніфіковану стратегію ідентифікації та контролю доступу (PAM), щоб гарантувати, що хмарні ідентифікатори не є скомпрометованими чи не розповсюджуються безконтрольно.
- Багатофакторну автентифікацію (MFA) для всього доступу або, як мінімум, використовуйте MFA для привілейованих облікових записів.
- Автоматизовані інструменти для моніторингу хмарних облікових записів, як на події безпеки (SIEM) так і в контексті аудиту налаштувань і привілеїв.

Принцип 2: Автоматизація налаштувань та перевірок в усіх хмарах

- Упродовж мого досвіду роботи я виявив, що переважна більшість інцидентів із безпекою в хмарі виникає внаслідок неправильної конфігурації або помилок клієнта, а не через зловмисників. У хмарному світі правильна конфігурація хмари так само важлива, як написання безпечного коду.
- Основні рекомендації щодо зменшення кількості неправильних налаштувань включають:
- Використовуйте як мінімум CSPM (систему управління безпекою в хмарі), щоб забезпечити безпечні конфігурації в усіх середовищах. Як правило кожна хмара надає власний CSPM.
- Використовуйте уніфіковану платформу безпеки для збору даних у всіх середовищах, наприклад Wazuh. Автоматизація хмарної безпеки стає все більш важливою частиною сучасних стратегій безпеки.

Принцип 3: Застосування DevSecOps і переміщення елементів керування вліво (shift-to-the-left)

- Коли розробники думають про хмарну безпеку, вони думають про технічні елементи керування, продукти з відкритим вихідним кодом, цікаві функції, контейнеризацію. Коли служби безпеки думають про засоби контролю, вони хочуть оцінити ризики. Вони хочуть знати, які засоби контролю ризиків безпеки існують, як їх автоматизувати і як їх підтверджувати.
- З цих причин дозволяти хмарним командам розробляти елементи керування безпекою не є хорошою практикою. Команди безпеки зобов'язані застосувати методи DevSecOps і забезпечити впровадження засобів контролю якомога раніше в процесі розробки. Хмарна безпека не повинна бути окремою організацією з власними інструментами та процесами. Команди мають бути об'єднані під єдину стратегію та використовувати інструменти, які дозволяють їм говорити однією мовою в усіх командах.
- Щоб «перейти вліво», вам потрібно:
- Сканувати свою інфраструктуру на наявність вразливих компонентів у конвеєрі розробки за допомогою систем аналізу складових компонентів (SCA).
- Стандартизувати динамічне тестування на вразливості (DAST). Перемістіть перевірки ліворуч, щоб можна було масштабувати у випадку необхідності розгортання готових рішень на декількох хмарах.

Принцип 4: Посилення безпеки даних

- Організаціям слід налаштувати власну систему пошуку і класифікації конфіденційних чи чутливих даних. З цим допоможе система класифікації даних.
- Вона не тільки проведе автоматизований аудит сховища документів на наявність конфіденційних даних, але і підготує організацію до використання системи запобігання витоку інформації (DLP). Т
- акі системи не повинні обмежуватись налаштуваннями CSPM, варто також зайнятись питанням захисту корпоративних ПК співробітників, через які здійснюється робота в хмарі. DLP повинна контролювати повний периметр можливого витоку: як на хмарі, так і на точці.

Принцип 5: Дотримання концепції нульової довіри (zero trust) для уніфікації стратегій

- Термін «нульова довіра» є зловживанням, але для наших цілей це означає нульову неявну довіру та повну видимість усієї поведінки об'єктів користувача після автентифікації та протягом життєвого циклу кожного сеансу. Це ключова вимога для хмари, але принцип нульової довіри слід запровадити також і для приватних хмарних середовищ.
- Щоб отримати повну користь від нульової довіри:
- Прийміть принципи нульової довіри як у загальнодоступних, так і в приватних хмарних середовищах, де це можливо.
- Поступово відмовляйтеся від довірених мереж. Принципи нульової довіри можуть бути рушійною силою для трансформації безпеки, що робить ваші програми більш безпечними в гібридних хмарних середовищах.