ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ ЗАСТОСУВАННЯ МЕТОДІВ БЕЗПЕКИ В ХМАРНИХ СЕРВІСАХ»

Виконав студент 6 курсу, групи БСДМ-62
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та
кібернетична безпека»
(шифр і назва спеціальності)
Квас Іван Олегович
(прізвище та ініціали)
Керівник Борсуковський Ю.В.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
“___”_____ 2022 року

15.12.2022 р.

		Строк виконання етапів магістерської роботи	Примітка
		26.09.2022 р.	
		.....2022 р.	
		.....2022 р.	
		.....2022 р.	
		.....2022 р.	
		.....2022 р.	
		15.12.2022 р.	

Квас І.О.

(підпис) прізвище та ініціали

Борсуковський Ю.В.

(підпис) прізвище та ініціали

РЕФЕРАТ

Текстова частина магістерської роботи: 56 сторінок, 8 рисунків, 1 таблиця, 26 джерел.

Об'єкт дослідження – процес захисту хмарних сервісів.

Предмет дослідження – технологія захисту хмарних сервісів.

Мета роботи – розробити варіант захищеного хмарного сервісу та рекомендації щодо застосування технології їх захисту.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу застосування захисту хмарного сервісу.

Різні IT рішення в наш час, без використання хмарних сервісів, важко уявити.

Дана технологія з кожним роком займає все більш вагоме місце в IT сфері, але разом із цим з'являють нові завдання перед обличчям кібербезпеки для захисту користувачів даних сервісів.

В роботі проаналізовано проблему забезпечення безпеки в хмарних сервісах. Проведено аналіз існуючих методів забезпечення захисту хмарних сервісів.

Розроблено та застосовано технологію методів безпеки хмарного сервісу.

Проаналізовано методи захисту хмарного сервісу.

Галузь використання – кібербезпека хмарних технологій.

ІНФОРМАЦІЙНА БЕЗПЕКА, КІБЕРБЕЗПЕКА, ХМАРНІ СЕРВІСИ, AWS, CLOUD SECURITY, GOOGLE CLOUD

ABSTRACT

Master's thesis: 56 pages, 8 figures, 1 tables, 26 sources.

Object of research – process of using cloud security methods.

Subject of research – technology of defending cloud services.

The aim of research – to develop a variant of secured cloud service and to develop a recommendations for the secured cloud service.

Research methods – elaboration of literature on the topic, analysis of operational documentation, international standards and their comparison, modeling of the process of securing the cloud.

Nowadays we cannot imagine different IT solution without cloud services.

This technology takes an increasingly important place in the IT sphere every year, but at the same time, new challenges are emerging in the face of cyber security to protect users of these services. This work analyzes the problem of ensuring security in cloud services. An analysis of the existing methods of ensuring the protection of cloud services was carried out.

The technology of cloud service security methods has been developed and applied.

Cloud service protection methods are analyzed.

Field of use – cybersecurity of cloud services.

INFORMATION SECURITY, CYBERSECURITY, CLOUD SERVICES, AWS, CLOUD SECURITY, GOOGLE CLOUD

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

SAAS – Software-as-a-Service

PAAS – Platform-as-a-Service

IAAS – Infrastructure-as-a-Service

SLA – Service-level agreement

КСЗІ – комплексна система захисту інформації

ЦОД – центр обробки даних

ПЗ – програмне забезпечення

API – Application Programming Interface

OLA – Operational Level Agreement

ITIL – Infrastructure Library

CASB – Cloud Access Security Broker

UBA – User Behavior Analytics

AWS – Amazon Web Services

IDC – International Data Corporation

DLP – Data Loss Prevention

COBIT – Control Objectives for Information and Related Technology

MFA – Multi-factor authentication

TLS – Transport Layer Security

SAML – Security Assertion Markup Language

XML – Extensible Markup Language

SSO – Single Sign-on

C2C – Cloud-to-Cloud

NAS – Network Attached Storage

EDR – Endpoint Detection and Response

IoC – Indicator of Compromise

SIEM – Security Information and Event Management

SSL – Secure Socket Layer

CLI – Command Line Interface

IAM – Identity an Access Management

IAP – Identity-Aware Proxy

VPN – Virtual Private Network

ВСТУП

Актуальність дослідження. Хмарні сервіси - це IT продукти, які розміщені і функціонують на фізичних ресурсах хмарних провайдерів. Основною перевагою хмарних сервісів є те, що вони доступні з будь-якого місця і будь-якого пристрою. Також важливим аспектом актуальності даної технології є оптимізація та уніфікація ресурсів, які використовують ці сервіси та гнучкість використання платформ, яких потербують сервіси.

Безпека такої технології займає одне з ключових місць при побудові і подальшому супроводженні, адже від цього залежить конкурентноспроможність бізнесу, який використовує дану технологію, а також захищеність даних окремих клієнтів, які використовують такі сервіси.

Вищесказане визначає актуальність теми даної магістерської роботи, основний зміст якої становить застосування методів безпеки в хмарних сервісах.

Об'єкт дослідження – процес безпеки хмарних сервісів.

Предмет дослідження – технологія захисту хмарних сервісів.

Мета роботи – розробити варіант захищеного хмарного сервісу та рекомендації щодо застосування технології захисту хмарних сервісів.

Наукові завдання:

дослідити сутність проблеми захисту хмарних сервісів;

встановити сутність завдань захисту хмарних сервісів;

проаналізувати існуючі технології захисту хмарних сервісів;

проаналізувати методи та засоби забезпечення захисту хмарних сервісів;

проаналізувати основні функції та принципи реалізації захисту хмарних сервісів.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання захищеного хмарного сервісу.

Практичне значення одержаних результатів полягає в розробці варіанта захищеного хмарного сервісу, а також у розробці рекомендацій щодо застосування технології захисту хмарних сервісів.

1 АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ХМАРНИХ СЕРВІСІВ

1.1. Призначення, структура, функції та умови функціонування хмарного сервісу

Як відмічається у [7], в загальному випадку хмара — це інструмент, який дає змогу IT-службі замовника максимально швидко, ефективно та з мінімальними капітальними витратами вирішувати ту чи іншу задачу. З кожним роком клієнти очікують від IT все більшої швидкості виводу та надання для себе нових сервісів, як внутрішніх, так і зовнішніх.

Тобто, використання хмарних сервісів значно скорочує витрати у використанні потрібного сервісу. Під витратами в даному контексті ми можемо мати на увазі як і часовий еквівалент так і людського ресурсу. Не можна також і не згадати про перевагу у стороні грошових ресурсів, адже використання такого рішення не потербує придбання окремого фізичного обладнання, а дозволяє орендувати потрібні потужності в хмарного провайдера. У разі безуспішності бізнес рішення компанія може просто відмовитись від оренди цих ресурсів і згорнути проект, при цьому не зробивши недоцільних витрат на придбання фізичного обладнання.

Виходячи з вищесказаного, хмарні сервіси - це про оптимізацію багатьох аспектів IT рішень.

За загальною інформацією, а також за [7], хмарні послуги можна поділяти на три типи - *IAAS, PAAS і SAAS.*

Доцільно спочатку розібрати тип **SaaS**. Розшифровується він як "Програмне забезпечення, як сервіс". За визначенням [2] його можна дефініціювати наступним чином: SaaS - це модель розгортання та реалізації програмного забезпечення, при якому постачальник (провайдер) розробляє додаток, ліцензує його, управляє ним, і надає споживачам доступ до ПЗ через Інтернет. Даний тип є найбільш поширений і вживаний як серед користувачів, так і IT спеціалістів. Він включає в себе надання уже готового рішення для клієнта, вимагаючи при цьому

мінімального втручання користувача в налаштування. Як і було зазначено вище, підписуючись на такий сервіс його керування може здійснювати навіть користувач з мінімальними навиками в сфері IT технологій і не потербувати втручання системного адміністратора для налаштування, всі ці задачі бере на себе постачальник послуги. Прикладами таких сервісів є Dropbox, Office 365, Google Drive, Evernote та інші.

Наступним типом є PaaS. Його розшифрування: "Платформа, як сервіс". Визначення за [3] дає нам наступне пояснення, що "Платформа, як сервіс" - це повноцінне середовище розробки і розгортання в хмарі з ресурсами, які дозволяють надавати будь-які хмарні додатки - від простих до передових рішень промислового класу. PaaS дозволяє запобігти витратам і труднощам пов'язаним з придбанням ліцензій на програмне забезпечення базової інфраструктури, ПЗ проміжного рівня, середовиз розробки і управління ними [3]. Опираючись на [7], можемо говорити про те, що цей тип розрахований в першу чергу на розробників. Така послуга включає в себе сервіси даних, репозиторії, інструменти автоматизованого розгортання, середовища тестування і тому подібні сервіси. Тобто, ви управляєте тільки додатками і службами, які розробляєте, а провайдер хмарних послуг займається обслуговуванням всього іншого. Прикладами таких сервісів - Google AppEngine, VMWare Pivotal Cloud Foundry, Red Hat's OpenShift, Heroku та інші.

І нарешті найскладнішим для кінцевого користувача є тип сервісу IaaS. Розшифровується він як "Інфраструктура, як сервіс". Таке рішення є найбільш гнучким у експлуатації, але разом і з тим найскладнішим у налаштуванні і супроводженні. Як сказано в [4], це різновид послуги хмарного сервісу, в якому постачальник надає основні ресурси для обчислень, зберігання і мережевого підключення по запиту з оплатою по мірі використання. IaaS позбавлює від витрат і складнощів пов'язаних з придбанням і адмініструванням фізичних серверів і інфраструктури центрів обробки даних. Кожний ресурс надається як окремий компонент служби, а оплата здійснюється за конкретний ресурс, доки у вас є в цьому потреба [4]. Інфраструктура, як послуга за своїми об'єктами та

характеристиками найбільш наближена до володіння власними фізичними серверами та віртуалізацією. Прикладами цієї моделі є AWS, Azure, Google Cloud.

Для візуалізації наведених вище даних найкраще підходять наступні зображення:

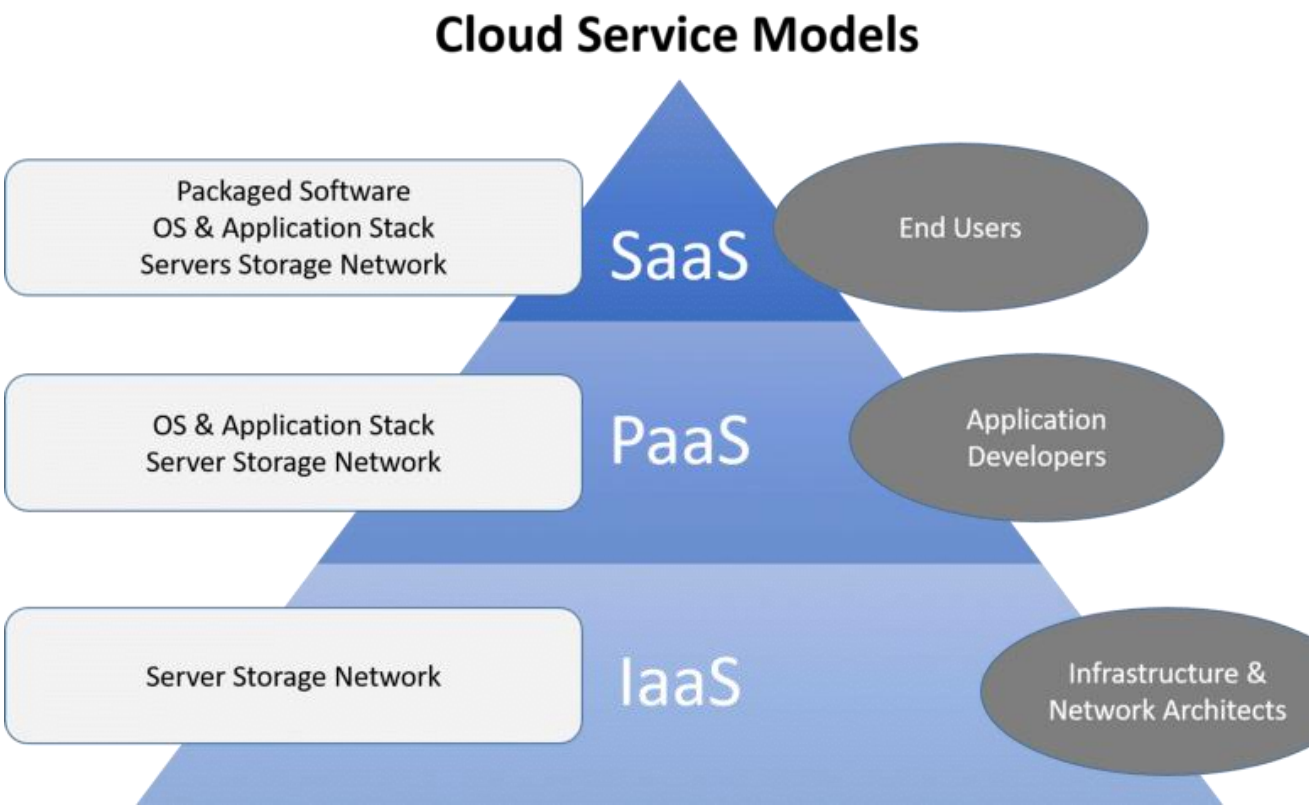

Рис. 1.1. Cloud Service Models

Також вирізняють різні моделі розгортання хмар, а саме приватна, публічна, гібридна, персональна хмара. Описати їх можна наступним чином:

— Приватна хмара — це хмарна інфраструктура, яка призначена для використання виключно однією організацією, що включає декілька користувачів (наприклад, підрозділів). Приватна хмара може перебувати у власності, керуванні та експлуатації як самої організації, так і третьої сторони (чи деякої їх комбінації). Така хмара може фізично знаходитись як в, так і поза юрисдикцією власника.

— Публічна хмара — це хмарна інфраструктура, яка призначена для вільного використання широким загалом. Публічна хмара може перебувати у власності, керуванні та експлуатації комерційних, академічних (освітніх та наукових) або державних організацій (чи

будь-якої їх комбінації). Публічна хмара перебуває в юрисдикції постачальника хмарних послуг.

— Гібридна хмара — це хмарна інфраструктура, що складається з двох або більше різних хмарних інфраструктур (приватних, громадських або публічних), які залишаються унікальними сутностями, але з'єднані між собою стандартизованими або приватними технологіями, що уможливлюють переносимість даних та прикладних програм (наприклад, використання ресурсів публічної хмари для балансування навантаження між хмарами).

— Персональна хмара — це приватна колекція цифрового контенту та додаткових сервісів які доступні з будь-якого пристрою і призначена для використання окремою особою (власником) та особами яким надано доступ. Це місце де користувач має можливість зберігати, синхронізувати, транслювати в потік та розповсюджувати приватний контент на сумісні платформи, екрани, з одного місцеположення в інше [9].

—

1.2. Аналіз проблеми забезпечення захисту хмарних сервісів

Звіт CloudPassage про хмарну безпеку AWS за 2021 рік показує, що неправильна конфігурація хмарних платформ (71 відсоток), викрадання конфіденційних даних (59 відсотків) і незахищені API (54 відсотки) є основними загрозами хмарній безпеці, з якими стикаються фахівці з кібербезпеки. Крім того, 95 відсотків респондентів підтвердили, що вони надзвичайно чи помірно стурбовані безпекою публічної хмари.

Ці побоювання, безумовно, виправдані. Згідно зі звітом IDC про стан безпеки в хмарі за 2021 рік, 79 відсотків опитаних компаній повідомили про порушення хмарних даних протягом останніх 18 місяців. Загальнодоступна хмарна інфраструктура як послуга (IaaS) може бути менш вразливою, ніж традиційні центри обробки даних, але це не означає, що вона позбавлена власного набору ризиків. Підприємства, які не хочуть бути частиною цієї статистики,

повинні розуміти та впроваджувати найкращі методи кібербезпеки, коли йдеться про їхню хмарну інфраструктуру [11].

За даними ресурсу Spectralops, опитування майже 2000 IT-спеціалістів показало, що хоча більшість (85%) підприємств вважають, що хмарні технології є критично важливими для інновацій, лише 40% справді мають політику безпеки. Крім того, майже половина респондентів, які використовують хмарну інфраструктуру, повідомили, що їхні інженери та розробники обходять або ігнорують хмарні політики безпеки та відповідності, що демонструє важливість технологій автоматизації та моніторингу.

За корпоративним середовищем, як і очікувалося, рушили зловмисники. У 2020 році кількість атак на хмарні сервіси зросла на 600%. За останні кілька років лише неправильна конфігурація хмари коштувала компаніям майже 5 трильйонів доларів і призвела до публікації понад 33 мільярдів записів користувачів. Тож не дивно знати, що до 2025 року очікується, що ринок хмарної безпеки зросте до понад 68 мільярдів доларів [14].

Хмарні обчислення є приваблими зважаючи на їх гнучкість та витрати, проте адміністратори хмарних сервісів мають мати глибоке розуміння процесів, які в них протікають, щоб мати змогу налаштувати політики та стандарти безпеки в поєднанні з обов'язковиими ролями та відповідальностю. На жаль, традийційні мережеві технології та механізми безпеки не можуть бути легко інтегровані до хмари [5]. Концепція "безпека хмари" відрізняється від терміну "безпека у хмарі". Вперше різниця була сформульована компанією Amazon для роз'яснення спільної відповідальності постачальників і клієнтів. Постачальники хмарних послуг зазвичай відповідають за фізичну та мережеву інфраструктуру хмарної служби. Клієнти - за налаштування доступу, парольну політику та інші питання, на які сервіс-провайдер вплинути не може. Ефективні рішення безпеки повинні захищати не тільки зв'язок між даними та користувачем, а й забезпечувати захист кожного підключення до кожного фізичного або віртуального пристрою в розподіленій інфраструктурі (чи між ними) [5].

Неправильні конфігурації продовжують залишатися найпоширенішою проблемою безпеки. Хакери можуть виявити неправильні конфігурації та використовувати їх для атаки.
Також хакери можуть отримати доступ до хмар через викрадені облікові дані, шкідливі контейнери та вразливості будь-якого програмного забезпечення. Також загрозоюми, яка надходить від хакерів на сьогодні є незаконний майнінг. Хакери використовують обчислювальну потужність хмар для майнінгу криптовалют, що буде досить дорого коштувати підприємству, оскільки рахунок сервіс-провайдер направить саме йому.

Не менш важливим є безпека окремих елементів хмари. Захист цих елементів від експлуатації, зловмисного програмного забезпечення та несанкціонованих змін — це складне завдання для адміністраторів хмар, оскільки навантаження постійно змінюється. Однак кожен елемент має бути видимим адміністратору хмари та керуватися політикою безпеки.

Традиційна безпека не може бути розгорнута на певних серверних платформах, але самі програми потрібно захищати так само надійно, як і інші частини інформаційної системи. Для багатьох компаній швидке та ефективне програмування та розгортання нових додатків є головними рушіями переходу до хмари. Але ці програми є потужними точками входу для загроз виконання веб-додатків, таких як введення коду, автоматизовані атаки та віддалені виконання команд. Витоки даних відбуваються в результаті того, що кіберзлочинці використовують найслабші ланки в інформаційній системі.

У багатьох організаціях впровадження хмари призводить до розширення можливостей для атаки у геометричній прогресії. Для усунення цих слабких ланок потрібно забезпечувати єдиний рівень безпеки, навіть коли інфраструктура постійно змінюється.

Оскільки інфраструктури розширюються і змінюються настільки швидкими темпами, важливо, щоб будь-які зміни в мережі здійснювалися в строгій відповідності із загальним планом безпеки. Вимога використовувати належні інструменти, політики і процедури безпеки до того, як будуть задіяні будь-які

нові ресурси, дозволяє адаптувати рішення безпеки до змін в інфраструктурі і в додатках. Для цього необхідно вибирати інструменти безпеки, які розуміють інфраструктуру, в якій вони будуть розміщені, і які зможуть забезпечити узгоджену роботу у всіх середовищах, гарантуючи дотримання політик і високу прозорість для безпечного запуску додатка і можливості безпечного підключення від центрів обробки даних до хмари [5].

Хмарні обчислення викликають занепокоєння щодо конфіденційності, оскільки постачальник послуг може отримати доступ до даних, які знаходяться в хмарі, у будь-який час. Це може випадково чи навмисно змінити чи видалити інформацію. Багато постачальників хмарних послуг можуть ділитися інформацією з третіми сторонами, якщо це необхідно для забезпечення правопорядку без ордера. Це дозволено в їхній політиці конфіденційності, з якою користувачі повинні погодитися, перш ніж почати користуватися хмарними сервісами. Рішення щодо конфіденційності включають політику та законодавство, а також вибір кінцевих користувачів щодо способу зберігання даних [9].

1.3. Аналіз існуючих технологій захисту хмарних сервісів

Захищений хмарний сервіс – це комплексне завдання, яке потербує комплексного рішення, отже єдиного правильного рішення для захисту не існує і така задача потербує для себе підходу з усих можливих сторін. Тому найперше рішення для захищеного хмарного сервісу є створення в хмарній інфраструктурі КСЗІ (Комплексна система захисту інформації). Якщо говорити у контексті міжнародних стандартів то це ISO/IEC 27001, ISO/IEC 27001, COBIT та інші. До складу КСЗІ входять заходи та засоби, які реалізують методи, механізми захисту інформації від несанкціонованих дій та несанкціонованого доступу до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав’язування хибної інформації, застосування закладних пристроїв чи програм, використання комп’ютерних вірусів та ін. [1].

Наступним кроком для забезпечення безпеки буде розміщення в ЦОД у відповідності до стандарту TIA-942, а також дотримання цим ЦОД всіх вимог для досягання найвищої класифікації по рівням від Uptime Institute, а саме показника TIER IV (найвищий показник на даний момент). У випадках використання моделей PaaS і SaaS, залежно від набору програмного забезпечення також обираються додаткові рішення покращення безпеки. Наприклад, використання методології OWASP для убезпечення вебдодатків у разі моделі SaaS, а також можливе і використання для PaaS моделей, наприклад для захисту API платформи.

Тобто, в залежності від вибору моделі, будуть різні рівні відповідальності сервіс провайдера. Але потрібно пам’ятати, що без забзпечення безпеки даних, які кінцевий користувач розміщує до хмарного сервісу захист завжди буде неповним, тому не менш важливим аспектом є правильна експлуатація хмарного сервісу користувачем в полі безпеки. Наступна ілюстрація гарно відображає розмежування відповідальності у відповідності до вибору моделі.

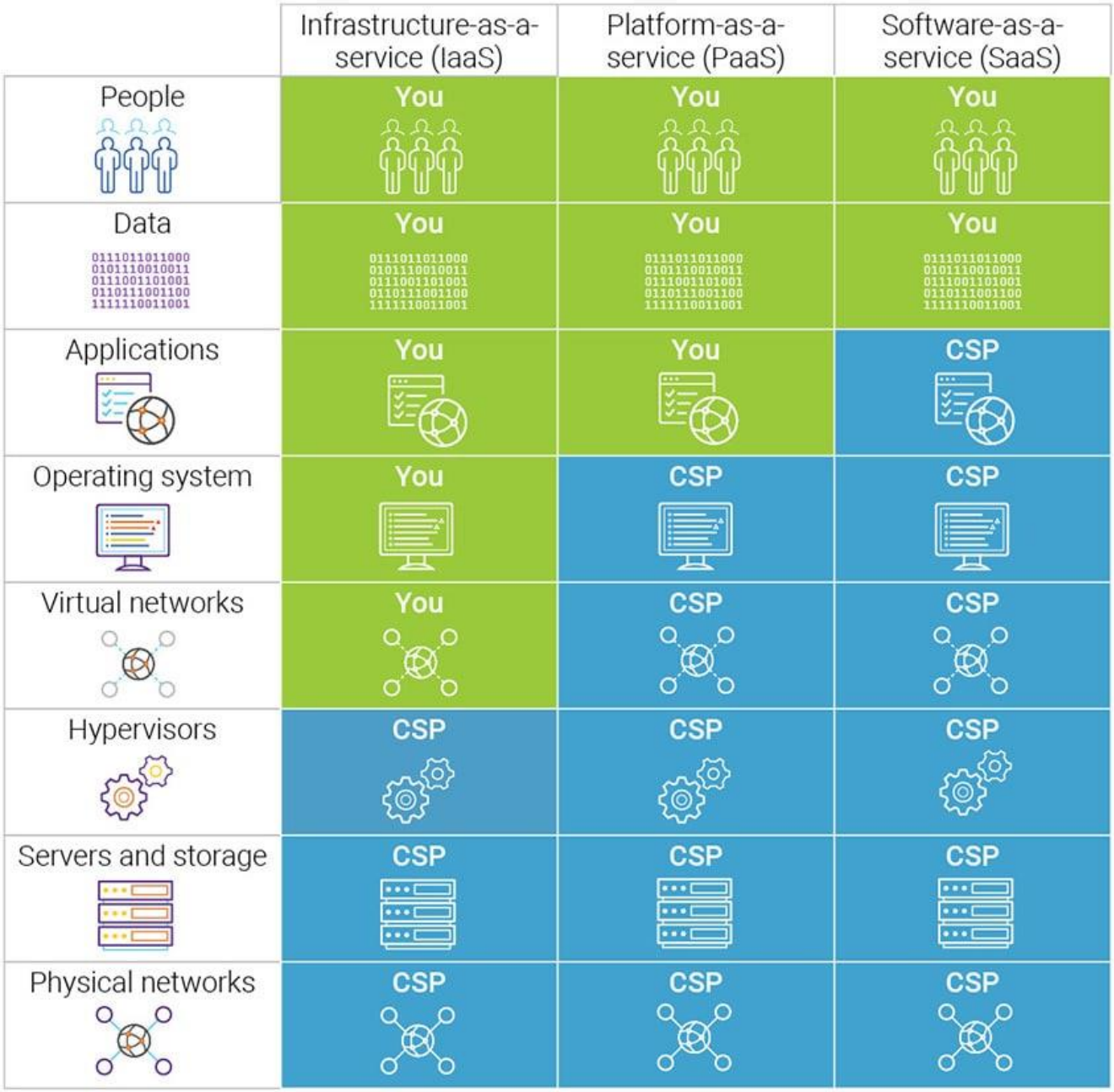

Рис. 1.2. Відповідальність у різних моделях хмари

2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ БЕЗПЕКИ В ХМАРНИХ СЕРВІСАХ

2.1. Дослідження методів безпеки в хмарних сервісах

Зважаючи на аналіз існуючих технологій захисту хмарних сервісів, можемо говорити, що потрібно чітко усвідомлювати, якої саме моделі потербує замовник (за рекомендаціями ITIL замовник і споживач – це два різні суб'єкти) при виборі хмарного сервісу, адже від цього залежить розуміння потрібної конфігурації безпеки як від сторони провайдера послуги, так і від сторони замовника. При визначенні такого розмежування варто керуватись таким показником, як SLA. Це угода між замовником і постачальником, яка визначає рівень послуг. Тобто, в SLA повинні входити детальний опис надаваного сервісу, у тому числі перелік параметрів якості, методів і засобів їх контролю, часу відгуку постачальника на запит від споживача, а також штрафні санкції за порушення цієї угоди. Для того, щоб дотримати SLA, постачальник послуг в свою чергу укладає операційну угоду про рівень послуг (OLA) з іншими внутрішніми підрозділами від яких залежить якість надання послуг [8].

Після визначення розмежування обов'язків і зон відповідальності між замовником і постачальником потрібно обирати правильні методи забезпечення безпеки сервісу з чітким поняттям того, що саме потрібно робити для досягнення потрібного рівня безпеки кожній із сторін.

Проте, в незалежності від типу сервісу, також можна сформувати і загальні положення, щодо вимог безпеки хмарного сервісу, які не градуються у відповідності до типу. Тому що в незалежності від типу хмарного сервісу кожна із сторін буде завжди мати один сталий рівень відповідальності. З боку користувача, він завжди буде відповідати за дані, які він розміщує на хмарному сервісі, незалежно від типу хмарного сервісу, так і постачальник завжди буде мати у своїй зоні відповідальності фізичну інфраструктуру хмари і ПЗ, яке здійснює віртуалізацію.

Слід розглянути наведені нижче критерії для вирішення основних проблем із хмарною безпекою щодо видимості й контролю над хмарними даними. Видимість хмарних даних — для повного перегляду хмарних даних потрібен прямий доступ до хмарної служби. Хмарні рішення безпеки досягають цього через підключення до хмарної служби через інтерфейс прикладного програмування (API). За допомогою підключення через API можна переглядати:

— Які дані зберігаються в хмарі.

— Хто використовує хмарні дані?

— Ролі користувачів з доступом до хмарних даних.

— З ким користувачі хмари обмінюються даними.

— Де розміщені хмарні дані.

— Де здійснюється доступ до хмарних даних і звідки вони завантажуються, зокрема з якого пристрою.

Далі, контроль над хмарними даними. Отримавши доступ до хмарних даних, застосуйте елементи керування, які найкраще підходять для вашої організації. Ці елементи керування включають:

- Класифікація даних — класифікуйте дані на кількох рівнях, наприклад конфіденційні, регульовані або публічні, коли вони створюються в хмарі. Після класифікації дані можуть бути зупинені на вході або виході з хмарної служби.
- Запобігання втраті даних (DLP) — запровадьте рішення DLP, щоб захистити дані від несанкціонованого доступу та автоматично вимкнути доступ і передачу даних у разі виявлення підозрілої активності.
- Елементи керування співпрацею — керуйте елементами керування в хмарній службі, як-от зниження дозволів на файли та папки для певних користувачів до редактора чи засобу перегляду, видалення дозволів і скасування спільних посилань.
- Шифрування — шифрування даних у хмарі можна використовувати для запобігання несанкціонованому доступу до даних, навіть якщо ці дані викрадено або викрадено.

Доступ до хмарних даних і додатків. Як і у випадку внутрішньої безпеки, контроль доступу є життєво важливим компонентом хмарної безпеки. Типові елементи керування включають:

- Контроль доступу користувачів — реалізуйте засоби керування доступом до системи та додатків, які гарантують доступ лише авторизованих користувачів до хмарних даних і програм. Посередник безпеки доступу до хмари (CASB) можна використовувати для забезпечення контролю доступу
- Контроль доступу до пристрою — блокуйте доступ, коли особистий неавторизований пристрій намагається отримати доступ до хмарних даних.
- Ідентифікація зловмисної поведінки — виявляйте зламані облікові записи та внутрішні загрози за допомогою аналітики поведінки користувачів (UBA), щоб уникнути зловмисного викрадання даних.
- Запобігання зловмисному програмному забезпеченню. Запобігайте проникненню зловмисного програмного забезпечення в хмарні служби за допомогою таких методів, як сканування файлів, білий список програм, виявлення шкідливих програм на основі машинного навчання та аналіз мережевого трафіку.
- Привілейований доступ — визначте всі можливі форми доступу, які привілейовані облікові записи можуть мати до ваших даних і програм, і встановіть засоби керування, щоб зменшити ризики.
- Забезпечення моніторингу ресурсів – контроль за всіма процесами, які відбуваються у хмарному середовищі.

Відповідність — Існуючі вимоги до відповідності та практики слід розширити, щоб включити дані та програми, що знаходяться в хмарі.

Оцінка ризиків — переглядайте та оновлюйте оцінки ризиків, щоб включити хмарні служби. Визначайте та вирішуйте фактори ризику, створені хмарними середовищами та провайдерами. Бази даних ризиків для хмарних провайдерів доступні для прискорення процесу оцінки [10].

Фізична безпека є ще одним стовпом хмарної безпеки. Це поєднання заходів для запобігання прямому доступу та збоям у роботі обладнання, розміщеного в центрі обробки даних вашого хмарного постачальника. Фізична безпека включає

контроль прямого доступу за допомогою захисних дверей, джерел безперебійного живлення, відеоспостереження, сигналізації, фільтрації повітря та частинок, протипожежного захисту тощо [13].

Мікросегментація стає все більш поширеною при впровадженні хмарної безпеки. Це практика поділу вашого хмарного розгортання на окремі сегменти безпеки, аж до індивідуального рівня окремих хмарних елементів. Ізолюючи окремі елементи хмари, ви можете застосовувати гнучкі політики безпеки, щоб мінімізувати будь-яку шкоду, яку може завдати зловмисник, якщо він отримає доступ [13].

Брандмауери наступного покоління – ще одна частина головоломки хмарної безпеки. Вони захищають ваші хмарні елементи за допомогою традиційних функцій брандмауера та новіших розширених функцій. Традиційний захист брандмауером включає фільтрацію пакетів, перевірку стану, проксі-сервер, блокування IP-адрес, блокування доменних імен і блокування портів. Брандмауери наступного покоління додають систему запобігання вторгненням, глибоку перевірку пакетів, контроль програм і аналіз зашифрованого трафіку для комплексного виявлення та запобігання загрозам [13].

Багатофакторна автентифікація гарантує, що лише авторизовані користувачі мають доступ до програм, даних і систем. Наприклад, можна використовувати пароль, OTP, SMS або мобільний додаток.

Більшість людей обирають слабкі паролі, які легко запам’ятовуються, і ніколи їх не оновлюють. Таким чином, адміністратори можуть мінімізувати цей ризик безпеки, використовуючи політики надійних паролів.

Це вимагає використання надійних паролів, термін дії яких закінчується. В ідеалі зашифровані маркери автентифікації, облікові дані та паролі зберігаються та передаються замість простих текстових облікових даних.

Використовуйте аналізатор журналів, щоб взаємодіяти з вашою системою оповіщення, підтримувати технологічні стеки вашої програми та мати інформаційну панель.

Це включає успішні та невдалі спроби входу, зміни пароля та інші події, пов’язані з обліковим записом. Крім того, автоматизований підхід може використовуватися для запобігання підозрілій і небезпечній діяльності [12].

2.2. Методи забезпечення безпеки хмарних сервісів

Для початку, варто розпочати з безпеки API інфраструктури, так як вона може бути надана самим хмарним провайдером, для взаємодії з хмарою користувачеві, так може бути присутня і в продукті, який розміщується.

Безпека API передбачає заходи та рішення для захисту цілісності API та запобігання зловмисним атакам. Це включає в себе процеси, які досліджують і пом’якшують ризики безпеки та вразливі місця в API. Якщо API залишаються незахищеними, це може бути використано хакерами для викрадення конфіденційних даних, завдаючи фінансової шкоди організаціям і завдаючи шкоди репутації.

У безпеці API використовуються різні методи, включаючи обмеження швидкості, аутентифікацію та авторизацію. Але крім цих методів, від підприємств також вимагається прийняття культури безпеки, яка охоплює весь процес розробки програмного забезпечення та API.

Для початку розберемо методи аутентифікації:

Відкрита авторизація (0Auth)

OAuth — це відкритий стандарт, який дозволяє стороннім службам, таким як Facebook або Twitter, отримувати дані облікового запису кінцевого користувача, не розкриваючи конфіденційні поля, наприклад паролі. По суті, він надає посередницьку послугу кінцевому користувачеві, надаючи службі маркер доступу, який підтверджує, що користувач дозволив надавати спільний доступ до інформації про обліковий запис.

Багатофакторна автентифікація (MFA)

MFA — це форма аутентифікації, яка вимагає більше одного методу перевірки облікових даних користувача. Наприклад, окрім пароля, цей метод також запитує пароль, надісланий користувачеві електронною поштою або

текстовим повідомленням, який потрібно підтвердити перед продовженням аутентифікації.

Безпека транспортного рівня (TLS)

TLS – це широко поширений протокол безпеки, який забезпечує автентифікацію, конфіденційність і цілісність даних між двома програмами, які взаємодіють між собою. Він використовується для веб-браузерів і програм, які передбачають безпечний обмін даними через мережу, наприклад під час сеансу перегляду, передачі файлів, передачі голосу через IP тощо.

Мова розмітки підтвердження безпеки (SAML).

SAML — це ще один відкритий стандарт, який використовується для безпечного обміну даними, включаючи ідентифікацію користувача, автентифікацію та авторизацію. Він реалізований за допомогою стандарту розширюваної мови розмітки (XML) і забезпечує основу для реалізації єдиного входу (SSO) [15].

Послідовно варто переходити до DLP (Data Loss Prevention) технології в хмарі, яка є не менш важливою за всі інші.

Захист від втрати даних у хмарі – це, загалом, процес захисту конфіденційної інформації в мережі від загрози втрати даних. Деякі описи йдуть далі та пропонують, що ці процеси та служби також повинні виявляти та класифікувати активи конфіденційних даних. У хмарі DLP часто є компонентом діагностики, а також практичним рішенням для захисту самих даних. Такі методи, як точне зіставлення даних і спеціалізована аналітика, можуть зіграти певну роль у захисті даних, які використовують компанії для функціонування, незалежно від того, чи це щоденні дані про транзакції, чи щось більш загальне, як-от аналіз бізнес-аналітики.

Інші визначення запобігання втраті хмарних даних зосереджені на різних загрозах для конфіденційних даних і способах їх усунення.

Розглядаючи всю роботу, виконану в DLP, важливо думати не лише про кібератаки, але й про ситуації, коли дані випадково видаляються. Наприклад, перезапис може бути проблемою з активністю хмарного сервера, де дані

стираються або втрачаються. Це не обов'язково наслідок шкідливих дій, а наслідок чогось іншого, наприклад, недостатньо організованої автоматизації.

Фахівці з безпеки також розрізняють тимчасову та постійну втрату даних. Коли дані тимчасово відсутні, їх часто описують як «недоступні». Зазвичай існують системні виправлення або процеси вирішення, які роблять дані знову доступними.

Тому, основоположним методом можна вирізнити такий метод, як резервні копії.

Коли йдеться про безпеку даних, резервне копіювання є дуже пріоритетним. Це проста концепція: резервне копіювання гарантує, що якщо набір даних буде втрачено або стане недоступним, резервне копіювання зможе безперешкодно ввімкнутись і забезпечить ту саму функцію. Резервне копіювання може бути різницею між тимчасовими збоями та постійними проблемами, які призводять до перебоїв у бізнес-процесах або, що ще гірше, до втрати прибутку [16].

В залежності від середовища, можливостей користувача і переслідуваних цілей є різні варіанти бекапування даних.

Один з них - резервне копіювання безпосередньо в публічну хмару. Одним із способів зберігання елементів хмари є дублювання ресурсів у загальнодоступній хмарі. Цей метод передбачає запис даних безпосередньо до хмарних провайдерів, таких як AWS або Microsoft Azure. Організація використовує власне програмне забезпечення для резервного копіювання, щоб створити копію даних для надсилання в службу хмарного зберігання. Потім служба хмарного зберігання надає місце призначення та безпечне зберігання даних, але не надає програму резервного копіювання. У цьому сценарії важливо, щоб програмне забезпечення резервного копіювання могло взаємодіяти зі службою хмарного зберігання даних. Крім того, з опціями публічної хмари IT-фахівцям може знадобитися переглянути додаткові процедури захисту даних.

Наступний метод – це резервне копіювання в постачальника послуг.

У цьому сценарії організація записує дані до постачальника хмарних послуг, який пропонує послуги резервного копіювання в керованому центрі

обробки даних. Програмне забезпечення для резервного копіювання, яке компанія використовує для надсилання своїх даних до служби, може надаватися як частина послуги, або служба може підтримувати окремі комерційно доступні програми резервного копіювання.

Також умовно новим видом резервного копіювання є резервне копіювання з хмари в хмару (C2C).

Ці послуги є одними з найновіших пропозицій на арені хмарного резервного копіювання. Вони спеціалізуються на резервному копіюванні даних, які вже зберігаються в хмарі, або даних, створених за допомогою послуги (SaaS), або даних, що зберігаються в хмарній службі резервного копіювання. Як випливає з назви, служба резервного копіювання з хмари в хмару копіює дані з однієї хмари в іншу. Служба резервного копіювання з хмари в хмару зазвичай містить програмне забезпечення, яке обробляє цей процес.

Ще одним із варіантів є використання хмарних онлайн-систем резервного копіювання.

Існують також апаратні альтернативи, які полегшують резервне копіювання даних у хмарну службу резервного копіювання. Ці пристрої є універсальними машинами для резервного копіювання, які включають програмне забезпечення для резервного копіювання та дисковий об’єм разом із резервним сервером. Такі пристрої забезпечують безперебійне (або майже таке) підключення до однієї або кількох хмарних служб резервного копіювання або хмарних провайдерів. Список постачальників, які пропонують пристрої для резервного копіювання з хмарними інтерфейсами, довгий, серед них Quantum, Unitrends, Arcserve, Rubrik, Cohesity, Dell EMC, StorageCraft і Asigra. Ці пристрої зазвичай зберігають найновішу резервну копію локально, а також надсилають її до хмарного постачальника резервних копій, щоб усі необхідні відновлення можна було виконати з локальної резервної копії, заощаджуючи час і витрати на передачу.

Коли використовується хмарна служба резервного копіювання, першим кроком є повне резервне копіювання даних, які потрібно захистити. Це початкове резервне копіювання іноді може тривати кілька днів, щоб завершити

завантаження через мережу через великий обсяг даних, які передаються. У стратегії резервного копіювання 3-2-1, коли організація має три копії даних на двох різних носіях, принаймні одну копію резервних копій даних слід надіслати до стороннього засобу резервного копіювання, щоб вона була доступною, навіть якщо локальна система недоступна.

Якщо обсяг даних у початковій резервній копії є значним, хмарна служба резервного копіювання може надати повний масив зберігання для процесу заповнення. Ці масиви, як правило, є невеликими мережевими сховищами (NAS), які можна відносно легко транспортувати туди-сюди. Після початкового заповнення через мережу створюється резервна копія лише змінених даних.

Також існують різні типи виконання резервних копій.

Повні резервні копії копіюють весь набір даних кожного разу, коли ініціюється резервне копіювання. Завдяки цьому вони забезпечують найвищий рівень захисту. Однак більшість організацій не можуть виконувати повне резервне копіювання часто, оскільки це може зайняти багато часу та забагато місця для зберігання даних.

Інкрементне резервне копіювання створює резервну копію лише тих даних, які були змінені або оновлені після останнього резервного копіювання. Цей метод економить час і простір для зберігання, але може ускладнити повне відновлення. Інкрементне резервне копіювання є поширеною формою хмарного резервного копіювання, оскільки воно використовує менше ресурсів.

Диференціальне резервне копіювання схоже на інкрементне резервне копіювання, оскільки містить лише змінені дані. Однак диференціальне резервне копіювання створює резервну копію даних, які змінилися після останнього повного резервного копіювання, а не останнього резервного копіювання в цілому. Цей метод вирішує проблему складного відновлення, яка може виникнути під час інкрементного резервного копіювання [17].

Дані резервного копіювання зазвичай шифруються перед передачею із системи клієнта до хмарної служби резервного копіювання та зазвичай залишаються зашифрованими в системах зберігання служби [17].

Як згадувалось раніше, шифрування є також одним з важливих методів безпеки.

Шифрування використовує розширені алгоритми для кодування даних, що робить їх безцільними для будь-якого користувача, який не має ключа. Авторизовані користувачі використовують ключ для декодування даних, перетворюючи приховану інформацію назад у читабельний формат. Ключі генеруються та передаються лише довіреним сторонам, чия особа встановлена та перевірена за допомогою певної форми багатофакторної автентифікації.

Хмарне шифрування призначене для захисту даних під час їх переміщення до хмарних програм і з них, а також під час їх зберігання в хмарній мережі. Це відомо як дані в дорозі та дані в спокої відповідно.

Шифрування даних під час передачі.

Значна частина даних, що переміщуються, автоматично шифрується за допомогою протоколу HTTPS, який додає до стандартного IP-протоколу рівень безпеки (SSL). SSL кодує всі дії, гарантуючи, що лише авторизовані користувачі можуть отримати доступ до деталей сеансу. Таким чином, якщо неавторизований користувач перехоплює дані, передані під час сеансу, вміст буде незрозумілим. Декодування здійснюється на рівні користувача за допомогою цифрового ключа.

Шифрування даних у стані спокою.

Шифрування даних для інформації, що зберігається в хмарній мережі, гарантує, що навіть якщо дані втрачено, викрадено або помилково поширено, вміст буде практично марним без ключа шифрування. Знову ж таки, ключі доступні лише авторизованим користувачам. Подібно до даних у дорозі, шифруванням/дешифруванням даних у стані спокою керує програмне забезпечення.

Алгортими шифрування на даний момент існують в різноманітних варіаціях і працюють в різноманітних варіантах роботи, проте є основні два розподілення на типи, які варто згадати. Це симетричне і асиметричне шифрування.

Симетричне шифрування: ключі шифрування та дешифрування однакові. Цей метод найчастіше використовується для масового шифрування даних. Хоча

реалізація загалом простіша та швидша, ніж асиметричний варіант, вона дещо менш безпечна, оскільки будь-хто, хто має доступ до ключа шифрування, може декодувати дані.

Асиметричне шифрування: використовує два ключі — відкритий і приватний — для кодування або декодування даних. Хоча ключі пов'язані, вони не однакові. Цей метод забезпечує підвищену безпеку, оскільки доступ до даних неможливий, якщо користувачі не мають загальнодоступного спільного ключа та закритого приватного ключа [18].

Метод контролю доступу для користувачів є не менш важливим у забезпеченні безпеки хмарних технологій, реалізувати його допомагає таке ПЗ, як CASB.

Брокер доступу до хмари (CASB) — це програмне забезпечення, розміщене в хмарі, або локальне програмне чи апаратне забезпечення, яке діє як посередник між користувачами та постачальниками хмарних послуг. Здатність CASB усувати прогалини в безпеці поширюється на середовища програмного забезпечення як послуги (SaaS), платформи як послуги (PaaS) та інфраструктури як послуги (IaaS). Окрім забезпечення видимості, CASB також дозволяє організаціям розширювати охоплення своїх політик безпеки з існуючої локальної інфраструктури на хмару та створювати нові політики для контексту хмари.

CASB стали життєво важливою частиною безпеки підприємства, дозволяючи компаніям безпечно використовувати хмару, одночасно захищаючи конфіденційні корпоративні дані.

CASB служить центром застосування політики, об'єднуючи кілька типів застосування політики безпеки та застосовуючи їх до всього, що бізнес використовує в хмарі, незалежно від того, який пристрій намагається отримати до нього доступ, включаючи некеровані смартфони, пристрої IoT або персональні ноутбуки .

Робота брокера доступу до хмари полягає в забезпеченні видимості та контролю над даними та загрозами в хмарі для задоволення вимог безпеки підприємства. Це робиться за допомогою триетапного процесу:

- Виявлення: рішення CASB використовує автоматичне виявлення для складання списку всіх служб хмари, а також того, хто ними користується.
- Класифікація: після виявлення повного масштабу використання хмари CASB визначає рівень ризику, пов'язаний з кожною з них, визначаючи, що це за програма, які дані містяться в програмі та як вони надаються.
- Виправлення: після того, як буде відомий відносний ризик кожної програми, CASB може використовувати цю інформацію, щоб установити політику щодо даних організації та доступу користувачів, щоб відповідати їхнім вимогам безпеки, і автоматично вживати заходів у разі порушення.

CASB також пропонують додаткові рівні захисту завдяки запобіганню зловмисному програмному забезпеченню та шифруванню даних [19].

Ще однією позицією методів безпеки в хмарному сервісі є аналіз поведінки користувачів (UBA).

Що таке аналіз поведінки користувачів? UBA, як можна здогадатися, це стратегія, яка використовується для моніторингу поведінки користувачів. Рішення UBA використовує вдосконалені методи машинного навчання для вивчення типових моделей поведінки. Якщо користувач діє способом, який відхиляється від цієї моделі, сповіщення в режимі реального часу буде надіслано адміністратору або буде ініційовано автоматичну відповідь. Рішення UBA буде агрегувати та співвідносити дані про події з кількох джерел і зберігати події в незмінній централізованій базі даних. Усі відповідні події будуть представлені на інтуїтивно зрозумілій інформаційній панелі, де їх можна шукати та фільтрувати лише кількома кліками.

Сьогодні найсучасніші рішення UBA можуть агрегувати дані з широкого спектру хмарних платформ за допомогою REST API або Syslog із більшості відомих платформ, таких як Dropbox, Office 365, Azure, AWS, G-Suite та багатьох інших. . Аналізуючи ці дані, рішення UBA може:

Позначити незвичні спроби входу, рішення UBA може виявляти та реагувати на численні невдалі спроби входу, а також спроби входу, які відбуваються поза звичайним робочим часом. Так само він може ідентифікувати спроби входу з незвичних IP-адрес або фізичних місць. Складне рішення UBA зможе розрахувати час між спробами входу та співвіднести цей час із відстанню між місцями входу, щоб визначити, чи були спроби входу від законного користувача.

Виявляти підозрілу активність файлів і папок, UBA може виявляти, сповіщати та реагувати на зміни, внесені до файлів і папок, що зберігаються в хмарі. Він може визначати, коли файли відкриваються, змінюються, переміщуються чи видаляються. Якщо, наприклад, відбулося несподіване збільшення кількості файлів, які завантажуються, можна підняти сповіщення та надіслати адміністратору. Крім того, що вони здатні виявляти моделі поведінки, які відрізняються від типових шаблонів використання, більшість рішень UBA здатні виявляти та реагувати на події, які відповідають попередньо визначеним пороговим умовам. Наприклад, якщо х кількість файлів було завантажено протягом заданого періоду часу, може бути подано сповіщення або може бути виконано спеціальний сценарій, який може вимкнути обліковий запис користувача, або запустити якийсь інший процес, щоб зупинити потенційну загрозу.

Виявлення змін конфігурації, в останні роки ми спостерігали низку витоків даних, спричинених неправильно налаштованими сегментами Amazon S3, де параметри безпеки за замовчуванням залишали їх відкритими для громадськості. Безсумнівно, важливо, щоб ми уважно стежили за будь-якими параметрами безпеки, які потенційно можуть призвести до розкриття конфіденційних даних. Окрім ретельного перегляду налаштувань безпеки перед завантаженням конфіденційних даних у хмару, ми також повинні мати можливість виявляти зміни конфігурації та реагувати на них, коли вони відбуваються. Рішення UBA забезпечить таку видимість, відстежуючи критичні зміни конфігурації на всіх платформах [20].

В контексті хмарної безпеки шкідливе програмне забезпечення нікуди не поділося і все ще становить велику загрозу безпеці ваших сервісів. З урахуванням вище згаданих методів, які також допомагають так чи інакше боротися зі шкідливим ПЗ, є ще також метод, який окремо націлиний на це, а саме безпосереднє сканування хмарних сервісів на наявність шкідливого програмного забезпечення.

Першим рішення у цьому методі буде захист своїх кінцевих точок, щоб виявити та усунути зловмисне програмне забезпечення, перш ніж воно потрапить у хмару.

Три функції виявлення EDR, які можуть допомогти відстежити та позбутися зловмисного програмного забезпечення, включають:

- Моніторинг підозрілих дій: EDR постійно відстежує кінцеві точки, створюючи «стек даних», які можна проаналізувати, щоб точно визначити будь-які індикатори компрометації (IoC).
- Ізоляція атаки: EDR запобігає бічному переміщенню атаки, дозволяючи ізолювати сегмент мережі, один пристрій або процес на пристрої.
- Реагування на інцидент: EDR може відобразити системні зміни, пов’язані зі зловмисним програмним забезпеченням, ретельно видалити зараження та повернути кінцеві точки до працездатного стану.

Навіть якщо ви виправили всі прогалини у своїй хмарній безпеці та використовуєте першокласний продукт EDR, реальність така, що зловмисне програмне забезпечення все одно може проникнути в хмару — і тому регулярне сканування хмарних сховищ є таким важливим.

Зайве говорити, що може бути складно відстежувати та контролювати всю активність у хмарних сховищах і поза ними, завдяки чому зловмисне програмне забезпечення легко ховається в шумі, коли воно пробирається до хмари. Ось де на допомогу приходить сканування хмарних сховищ.

Сканування хмарних сховищ – це саме те, як це звучить: це спосіб перевірити наявність зловмисного програмного забезпечення в програмах для хмарних сховищ, таких як Box, Google Drive і OneDrive. І хоча більшість додатків для хмарних сховищ мають можливості сканування зловмисного програмного забезпечення важливо розуміти, що непоганим варіантом є використання двох різних сканерів хмарного сховища. Це є чудовою другою лінією захисту для хмарного сховища, тому що дуже ймовірно, що основний сканер не зможе виявити хмарне зараження зловмисним програмним забезпеченням, яке виловить ваш другий сканер [21].

І ще один з більш специфікованих методів, але від того не менш важливий – це загальний моніторинг ресурсів, які використовуються. Такий метод дає можливість запобігати навіть не тільки явним порушенням політик безпеки, а і помилками та ситуаціям, які можуть виникнути в ході експлуатації, а також створити додаткову опору до всих інших згаданих методів.

Рішення для моніторингу в хмарі може бути вбудовано в інфраструктуру хостингу хмарного сервера (наприклад, CloudWatch від AWS), або вони можуть бути сторонніми рішеннями, які додаються до існуючого середовища . Організації також можуть здійснювати хмарний моніторинг за допомогою існуючих інструментів керування безпекою.

Як і SIEM, хмарний моніторинг безпеки працює шляхом збору даних журналу на серверах. Розширені рішення хмарного моніторингу аналізують і співвідносять зібрані дані на наявність аномальної активності, а потім надсилають сповіщення та активують реагування на інциденти. Хмарна служба моніторингу безпеки зазвичай пропонує:

- ✓ Видимість. Перехід до хмари за своєю суттю знижує видимість організації в її інфраструктурі, тому інструменти безпеки хмарного моніторингу повинні мати чіткий функціонал для відстеження поведінки програм, користувачів і файлів для виявлення потенційних атак.

- ✓ Масштабованість. Хмарні інструменти моніторингу безпеки повинні мати можливість контролювати великі обсяги даних у різних розподілених місцях.
- ✓ Аудит. Організаціям важко управляти та відповідати вимогам відповідності, тому хмарні інструменти моніторингу безпеки повинні надавати надійні можливості аудиту та моніторингу.
- ✓ Постійний моніторинг. Розширені рішення для моніторингу безпеки в хмарі повинні постійно відстежувати поведінку в режимі реального часу, щоб швидко виявляти зловмисну активність і запобігати атаці.
- ✓ Інтеграція. Щоб максимізувати видимість, рішення хмарного моніторингу в ідеалі має інтегруватися з існуючими службами організації, такими як Microsoft 365 і G Suite наприклад, рішення безпеки окремих елементів хмари (тобто Crowdstrike і VMware Carbon Black) і служби ідентифікації та автентифікації (тобто Duo і Okta).

2.3. Інструменти для впровадження безпеки хмарного сервісу

Варіативність інструментів, які можна використовувати для захисту хмарного сервісу, на сьогодні представляє доволі широкий спектр, навіть не зважаючи на той факт, що ця технологія є відносно нова та складна у реазілації.

Різні інструменти можуть відповідати як окремим вимогам і чітко виконувати поставлену задачу, так і бути повним мультизадачним середовищем, яке може виконувати одразу багато функцій. Інструментарні рішення також не обмежені тільки платними продуктами, існує також велике різноманіття інструментів, які створені і розробляються спільнотами на засадах відкритого вихідного коду і того, що цей продукт поширюється під безкоштовною ліцензією. Для того щоб виокремити переваги і недоліки кожного із них варто переглянути табличку, приведену нижче.

Таблиця 2.1.

Програмні рішення забезпечення безпеки хмарних сервісів

Назва продукту	Open Source	Кроссплатформенність	Відповідність задачам	Можливість самостійного розгортання
Osquery	Так	Так	Аудит, моніторинг	Так
GoAudit	Так	Ні, тільки Linux	Аудит, моніторинг	Так
OSSEC	Так	Так	Моніторинг, система виявлення вторгнень	Так
Syncthing	Так	Так	Створення резервних копій	Так
BetterCloud	Ні	Так	DLP	Ні
Beagle Security	Ні	Так	Безпека API	Ні
Netskope	Ні	Так	CASB	Ні
Redstor	Ні	Ні	DLP	Ні
Elastic	Ні	Так	Аналітика, моніторинг	Так

Як бачимо, варіативність окремих інструментів доволі велике і їхній функціонал, так чи інакше, може перехрещуватись, проте, крім самостійних інструментів, у провайдерів хмарних послуг існують також одразу цілі інтеграції і набори інструментаріїв, які можуть виконувати всі функції, що і наведене вище ПЗ. При цьому, додатково забезпечети один із методів не є проблемою, тому що розгортання окремого інструменту у зв’язці з готовими рішеннями постачальника

є поширеною практикою. Різні провайдери, такі як Microsoft Azure, AWS чи Google Cloud, надають широкий спектр можливостей не тільки для розгортання підготованих рішень, а і можливості додаткових налаштувань безпеки не виходячи за межі платформи.

Розберемо інструменти, які надає такий постачальник, як Google, для своєї хмари, так як практична частина виконання цієї роботи, буде здійснена саме на цій інфраструктурі.

У випадках відсутності платної підписки, чи акаунту до організації багато інструментів є недоступні для користувача, проте навіть попри це є варіанти вибору з поміж доступних.

Найперший інструмент, доступний на цій платформі – це менеджер сертифікатів. Цей інструмент допомагає користувачам створювати та керувати SSL сертифікатами, щоб забезпечувати безпечене з'єднання з сервісами, які знаходяться в хмарі Google. Управління можна здійснювати як з використанням графічного інтерфейсу, так і через CLI.

Наступний доступний інструмент – це reCAPTCHA. Цей інструмент можна інтегровувати до сервісів, які використовуються в хмарі. Його ціль – це захист вашого сервісу від поширених веб-атак, сканування і неавторизованих дій зловмисних автоматизацій.

Після цього слідкує інструмент під назвою Asset Inventory. Створений від для відстежування активності пов'язаної з вашими хмарними сервісами.

Cloud Asset Inventory надає послуги інвентаризації на основі бази даних часових рядів. Ця база даних зберігає п'ятитижневу історію метаданих активів Google Cloud. Cloud Asset Inventory дозволяє шукати метадані ресурсу за допомогою спеціальної мови запитів, експортувати всі метадані активів за певну позначку часу, або експортувати історію змін подій протягом певного періоду часу, слідкувати за змінами активів, підписавшись на сповіщення в реальному часі, аналізувати політику IAM, щоб дізнатися, хто до чого має доступ [23].

Далі знаходиться так званий сканер безпеки. Web Security Scanner виявляє вразливі місця у ваших веб-додатках, які використовуються на платформі. Він

сканує програму, переходячи за всіма посиланнями в межах початкової URL-адреси, і намагається використати якомога більше користувацьких даних і обробників подій. Наразі Web Security Scanner підтримує лише загальнодоступні URL-адреси та IP-адреси, які не захищені брандмауером.

Web Security Scanner розроблено, щоб доповнити існуючі безпечні процеси проектування та розробки. Щоб не відволікати помилковими спрацьовуваннями, Web Security Scanner не надсилає звітів і не відображає сповіщень із низьким рівнем надійності. Це не замінює перевірку безпеки вручну та не гарантує, що програма не містить недоліків безпеки [24].

Далі існує дуже цікавий інструмент під назвою Access Approval. Створений він для того, щоб при доступі підтримки Google, або їх інженерів, до ваших даних, ви надавали на це дозвіл. Але цей продукт доступний тільки з відповідним планом підтримки.

Також є такий інструмент, як Cloud Key Management Service. Виконує він свої задачі відповідно до своєї назви, а саме управління криптографічними ключами та проведення різних операцій з ними.

Google попіклувався також про зберігання вразливих даних, тобто паролів, сертифікатів, ключів API, створивши інструмент під назвою Secret Manager.

Наступним є доволі потужний інструмент, а саме IAP. IAP дозволяє встановити центральний рівень авторизації для додатків, доступ до яких здійснюється через HTTPS, тож можна використовувати модель контролю доступу на рівні програми замість того, щоб покладатися на брандмауери на рівні мережі.

Політика IAP масштабується у проекті. Можна централізовано визначати політики доступу та застосовувати їх до всіх своїх програм і ресурсів. Коли призначається спеціальна група для створення та впровадження політик, то ви захищаєте свій проект від неправильного визначення або впровадження політики в будь-якій програмі [25].

Ще Google пропонує своїм користувачам інтсрумент DLP. Працює він наступним чином.

Завдяки понад 150 вбудованим інфо-типам Cloud DLP дає змогу сканувати, виявляти, класифікувати та створювати звіти про дані практично з будь-якого місця. Cloud DLP має вбудовану підтримку для сканування та класифікації конфіденційних даних у Cloud Storage, BigQuery та Datastore, а також API потокового вмісту для підтримки додаткових джерел даних, спеціальних робочих навантажень і програм.

Cloud DLP надає інструменти для класифікації, маскування, токенізації та трансформації конфіденційних елементів, щоб допомогти краще керувати даними, які збираються, зберігаються або використовуються для бізнесу чи аналітики.

Завдяки підтримці структурованих і неструктурованих даних Cloud DLP може допомогти зберегти корисність ваших даних для приєднання, аналітики та штучного інтелекту, одночасно захищаючи необроблені конфіденційні ідентифікатори. А також можна вимірювати ризик повторної ідентифікації в структурованих даних. Властивим для цього інструменту також є те, що він може взаємодіяти з квазіідентифікаторами. Квазіідентифікатори – це частково ідентифікаційні елементи або комбінації даних, які можуть пов’язуватись з окремою особою чи дуже невеликою групою. Cloud DLP дозволяє вимірювати статистичні властивості, такі як k-anonymity та l-diversity, розширюючи вашу здатність розуміти та захищати конфіденційність даних [26].

Окрім всього цього, існують можливості та набори інструментів, які не є прямими вказівниками безпеки, але так чи інакше впливають на неї. Це і можливість побудови VPC (Virtual Private Cloud Network) мережі, які дозволяють будувати захищені віртуальні мережі в хмарній інфраструктурі, включаючи і можливості фільтрування брендмауером таких мереж, і можливості створення бекапів, у вигляді снепшотів віртуальних елементів, ба навіть засоби моніторингу та реагування на інциденти. Також Google надає розширені можливості управління, знову таки завдячуючи великому різноманіттю API, готових рішень управління і все це зібрано в одному місці, що значно полегшує управління, розгортання і експлуатацію хмарних сервісів.

3 РОЗРОБЛЕННЯ ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ХМАРНОГО СЕРВІСУ

3.1. Використання технології застосування методів безпеки хмарних сервісів

Розглянемо наступну схему, в якій буде розміщено три робочі хмарні елементи. Перший – це сервер, на якому розміщений самостійний програмний продукт, другий – це елемент, на якому розміщений сервер API, для взаємодії з програмним продуктом і третій елемент – це база даних, яка потрібна для використання самим програмним продуктом.

Розміщені вони в хмарі в наступних інтерпретаціях: сервер API і сервер продукту – це самостійні віртуальні сервери, на яких зі сторони постачальника було підготовано тільки обчислювальні потужності і операційна система, подальше розгортання середовища, розміщення і експлуатація програмних рішень уже відбувались на стороні замовника. Також, варто відмітити, що хоч і постачальник надає підготовону операційну систему, проте він не здійснює подальше її супроводження.

Трохи інша ситуація з базою даних. Вона була розгорнута засобами, які уже надаються постачальником послуг, отже в схемі відповідальності цього сервісу, постачальник відповідає не тільки за обчислювальні ресурси, а і також за середовище та додаток, який вона надає, в даному випадку – це MySQL база даних. Тобто, фактично у нас є три послуги, дві з яких відповідають типу IaaS та одна типу SaaS.

Перейдемо тепер безпосередньо до застосування наданих методів безпеки для хмарних сервісів. Перше, що варто відмітити – це побудова мережевої взаємодії між ціми сервісами. Google Cloud надає можливість використання не тільки публічних IP адрес, а й також внутрішні приватні мережі датацентрів. Тому увесь мережевий трафік між цими сервісами не виходить за межі хмари і маршрутизується по приватній мережі.

Розглянемо ближче інтерфейси самих сервісів і їх можливості. Ось так виглядає інтерфейс управління сервісом бази даних.

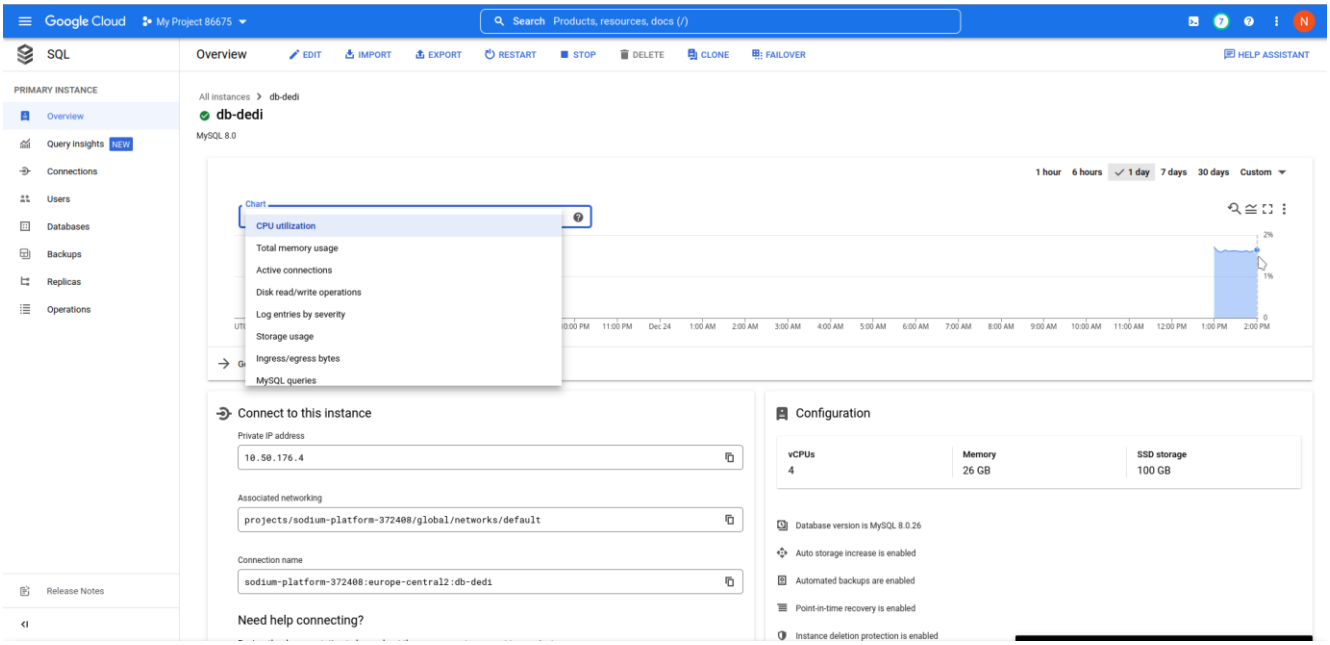

Рис. 3.1. Інтерфейс сервісу бази даних

Як бачимо, в базовому функціоналі уже закладено чимало портібних механізмів. Це і візуалізація зібраних метрик моніторингу (самі метрики також розроблені і засосовані постачальником), різноманіття зібраних даних також дозволяє керувати не тільки загальними процесами, а і помічати інцидетни, які так чи інакше мають відношення до безпеки. За замовчування, постачальник також встановлює створення бекапів, які зберігаються безпосередньо у нього. Також резервування бази даних відбувається і сторонніми інструментами, зберігаючи дані на NAS.

Для екземплярів також було створено графік створення бекапів. Зі сторони хмарних рішень – це створення знімків віртуальних машин. Графік такий: кожного дня, в період між четвертою та п’ятою годиною ранку, створюється п’ять копій, які змінюються в режимі ротації, тобто перезаписуючи останню.

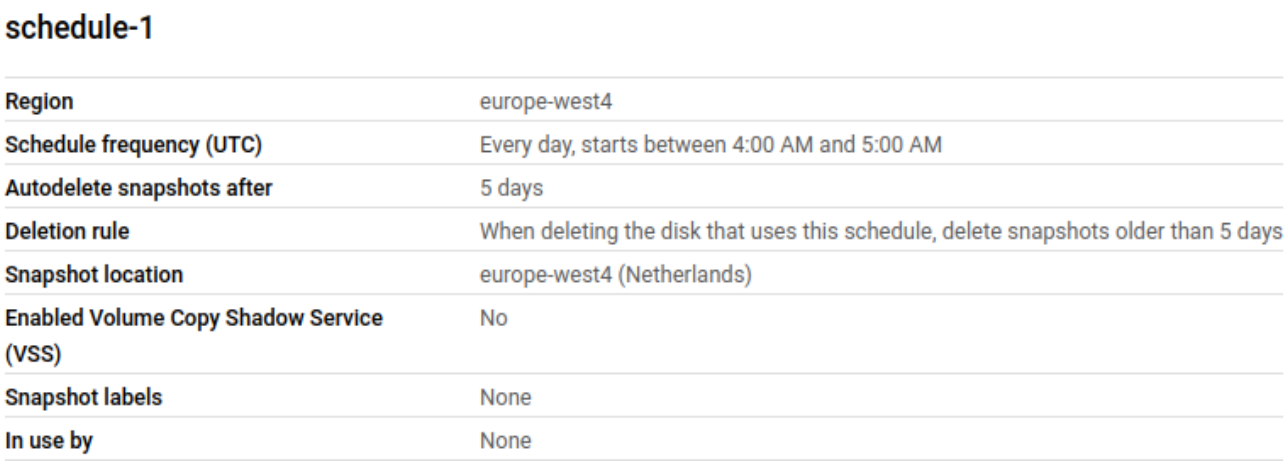

Рис. 3.2 Графік бекапів

Провайдер надає можливість також убезпечити публічні з'єднання, встановивши прямо з інтерфейсу SSL сертифікат для шифрування з'єднань, що безпосередньо і було проведено, також було відключено можливість з'єднуватись по незашифрованим каналам зв'язку.

Також було створено користувачів для бази даних, а саме користувача для серверу з продуктом та окремих користувачів через інструмент IAM, яким потрібне пряме з'єднання з базою даних для проведення технічних робіт. Ще в IAM було створено окремого користувача для з'єднання екземплярів з Google Cloud Storage.

Кроком слідуючим за минулим було налаштування веб сканеру для розміщеного продукту в хмарі. Налаштований він був з указанням доменого імені, яке відповідало IP адресі серверу з продуктом, сканування здійснюється автоматично раз в тиждень, у разі додаткової потреби можна запустити сканування вручну.

Рис. 3.3 Налаштування вебсканеру

Для захисту продукту безпосередньо в окремих уразливих місцях використано інструмент reCAPTCHA. Її було додано на сторінку реєстрації продукту.

Що не менш важливо, для управління атрибутами службових користувачів, які знаходяться поза межами поля авторизації Google, використано такі два інструменти як Google KMS, а також Google Secret Manager. Перший використовується для зберігання ключів шифрування атрибутів користувачів, другий для безпосередньо зберігання атрибутів.

Для екземплярів було налаштовано мережеві фільтри у відповідності до вимог безпеки і експлуатації. Було відкрито доступ до екземпляру з продуктом зі світу за портами, які використовуються протоколом http та https. Для екземпляру з API було створено правила, які дозволяють підключатись тільки визначеним публічним IP адресам, які є службовими. Для бази даних був відкритий порт, який використовується для підключення до неї з приватної мережі, яку використовують два інші екземпляри, а також виключення для деяких публічних IP адрес, з якими підключаються службові програми.

Управління всіми екземплярами здійснюється засобами хмари, тому дозволяти доступи для управління від віддалених серверів не потрібно.

Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network	Logs	Hit count	Last
api-service	Ingress	api-service	IP ranges: 212.2(	tcp:8000	Allow	1000	default	Off	–	–
http-prod	Ingress	http-prod	IP ranges: 0.0.0.(	tcp:80, 443	Allow	1000	default	Off	–	–
mysql-con	Ingress	mysql-con	IP ranges: 10.18(	tcp:3306	Allow	1000	default	Off	–	–
mysql-pub	Ingress	mysql-con	IP ranges: 212.2(	tcp:3306	Allow	1000	default	Off	–	–

Рис. 3.4 Правила мережевого фільтру

Одним з найпотужніших інструментів, який було використано став Cloud DLP. Завдяки йому було впроваджено періодичне сканування бази даних.

Схема його роботи наступна. Дамп бази даних робиться з періодичністю раз в 3 три дні і розміщається в так званий «бакет», який представляє собою контейнер для зберігання даних у середовищі Google Cloud Storage. Cloud DLP сканує цей дамп на наявність чутливих даних і видає нам звіт.

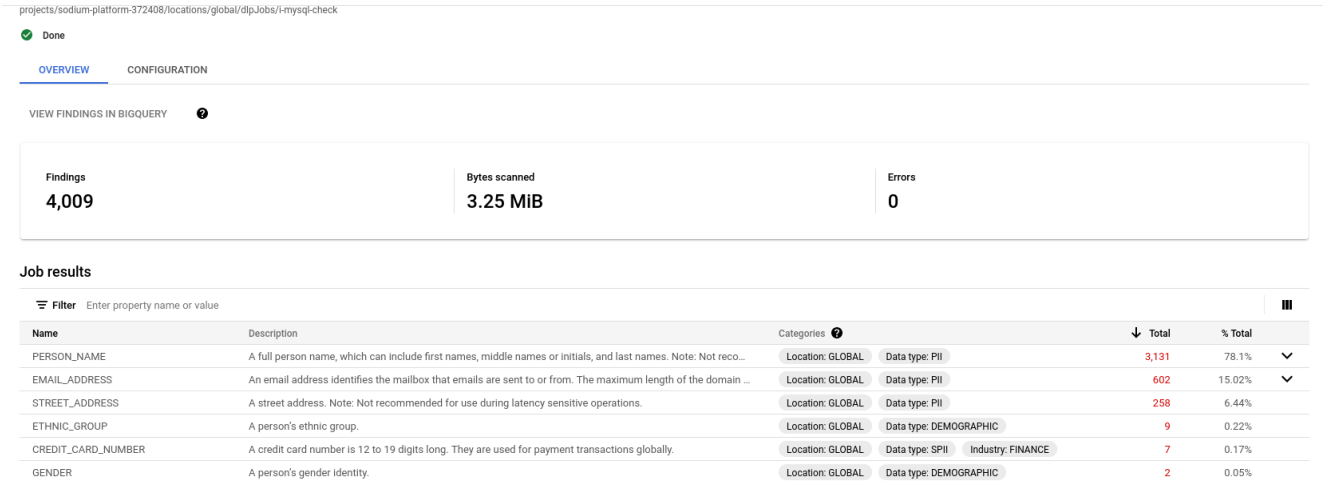

Рис. 3.4 Результати роботи DLP

Щодо додаткових дій, які проводить зі знайдеми даними механізмом DLP, встановлюється конфігурацієїю, в моєму випадку це резервування файлів дампів баз даних, в яких містяться чутливі дані, а також зберігання до так званого BigQuery. Додатково надходять сповіщення на електронну пошту та всі результати відправляються до центру моніторингу хмари.

Також Google надає можливість не тільки використовувати підготовлені ним же патерни для даних, а і створювати свої, що значно розширює можливості для тонкого калібрування цього інструменту. Наприклад, було додано патерн реагування на службові домени в даних, для того щоб службова інформація завжди була зарезервована. Наведений нижче скріншот відображає приклад конфігурації для такого патерну. В налаштуванні типу чутливих даних можна вказувати не тільки окремі регулярні вирази, а і використовувати набори слів і навіть цілі словники, чи навіть словники з бази даних BigQuery.

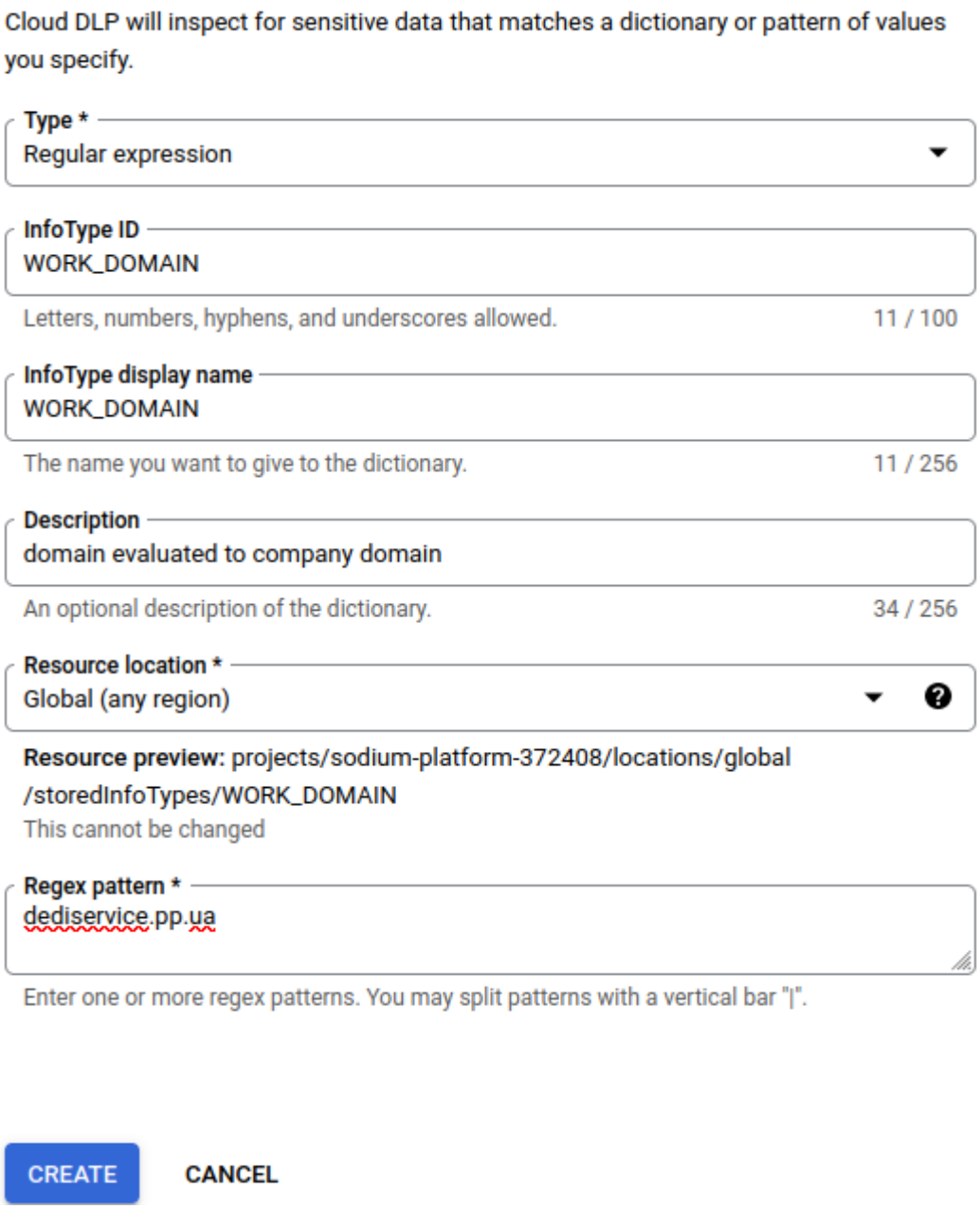

Рис. 3.5 Приклад налаштувань власного типу чутливих даних

3.2. Результати реалізації технології застосування методів безпеки хмарних сервісів

У даній реалізації досліджено методи безпеки хмарних сервісів та їх практична реалізація на прикладі постачальника Google. Підходи і рішення можуть бути дуже різні, проте всіх їх об’єднує один фактор – вони так чи інакше виконують завдання з забезпечення безпеки. З появою цілих інтеграцій завдання захисту хмарних сервісів відтепер можуть легко реалізовуватись з використанням інструментарію наданого постачальником, відкидаючи потребу в самостійному

налаштуванні окремих стеків технологій.

В реалізації безпосередньо забезпечено мережеву безпеку хмарних сервісів, з використанням внутрішніх мереж, мережевих фільтрів, які є частиною хмари. Безпека самих додатків, які використовуються в хмарі була забезпечена з використанням наданих хмарних інструментів: використання reCAPTCHA та сканеру уразливостей. Для сервісів забезпечений моніторинг знову ж таки у вигляді створених рішень від безпосередньо самого постачальника. Для забезпечення резервування даних було використано як рішення постачальника так і сторонні рішення. Було застосовано методи криптографії для захисту з'єднань з базою даних, а також для зберігання атрибутів доступу службових користувачів. Також було реалізовано розмежування доступів і ролей з інструментом IAM. Найбільш важливим методом, який було використано став DLP. Завдяки йому було створено механізм для обробки і зберігання чутливих даних, який забезпечує їхню безпеку.

ВИСНОВКИ

В магістерській роботі отримано наступні наукові так науково-практичні резльтати:

1. Досліджено готові програмні рішення захисту хмарних сервісів від одного з постачальників таких, а саме Google Cloud, які дають можливість забезпечети захист хмарних сервісів на основі традиційних методів безпеки інтерпретованих в хмарне середовище.
2. Проаналізовано безпосередньо самі інструменти, які надають захист, а саме Cloud DLP, reCAPTCHA, хмарний мережеві фільтри, хмарні резервування даних.
3. Використано на практиці вище згадані інструменти, розглянутий їхній основний функціонал і можливості в контексті мети створення захищеного хмарного сервісу.
4. Безпосередньо застосовано методи захисту хмарних сервісів за допомогою практичного використання інструментів наданих постачальником хмарних послуг.
5. Самі методи забезпечення не обмежуються інструментами, які надаються провайдером. Деякі з них можуть бути застосовані тільки за дотриманням певних комерційних умов, проте існують також і сторонні інтеграції для створення захищеного периметру, якщо такі потербує сама система. Такі інтеграції також можуть бути використані, якщо засобів, наданих провайдером, не вистачає для реалізації, інфраструктура хмарних сервісів також дозволяє і це. Проте, такі ситуації виникають не завжди і зазвичай можливостей хмарних провайдерів вистачає для забезпечення безпеки в хмарному сервісі замовника.

ПЕРЕЛІК ПОСИЛАНЬ

1. Поради (рекомендації) щодо створення КСЗІ в ІТС, які використовуються для надання послуг доступу до мережі Інтернет [Електронний ресурс] – Режим доступу: https://cip.gov.ua/ua/news/poradi-rekomendaciyi-shodo-stvorennya-kszi-v-its-yaki-vikoristovuyutsya-dlya-nadannya-poslug-dostupu-do-merezhi-internet .

2. Що таке програмне забезпечення як послуга (SaaS)? [Електронний ресурс] – Режим доступу: https://cbto.com.ua/library/saas.

3. Microsoft Azure. Що таке PaaS? Платформа як послуга. [Електронний ресурс] – Режим доступу: https://azure.microsoft.com/ru-ru/resources/cloud-computing-dictionary/what-is-paas.

4. Microsoft Azure. Що таке IaaS? Інфраструктура як послуга [Електронний ресурс] – Режим доступу: https://azure.microsoft.com/ru-ru/resources/cloud-computing-dictionary/what-is-iaas.

5. Хмарна безпека: ключові поняття, загрози та рішення [Електронний ресурс] – Режим доступу: https://sgs4business.com/news/khmarna-bezpeka-kliuchovi-poniattia-zahrozy-ta-rishennia.html.

6. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 1.1-003-99 [Електронний ресурс] – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=102106&cat_id=46556&ctime=1344502446343.

7. Види хмарних сервісів та приклади їх використання [Електронний ресурс] – Режим доступу: https://denovo.ua/blog/vidi-hmarnih-servisiv-yakij-obrati-ta-oglyad-hmarnih-provajd-8

8. Угода про рівень послуг [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/%D0%A3%D0%B3%D0%BE%D0%B4%D0%B0_%D0%BF%D1%80%D0%BE_%D1%80%D1%96%D0%B2%D0%B5%D0%BD%D1%8C_%D0%BF%D0%BE%D1%81%D0%BB%D1%83%D0%B3 .

9. Хмарні обчислення [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/%D0%A5%D0%BC%D0%B0%D1%80%D0%BD%D1%96_%D0%BE%D0%B1%D1%87%D0%B8%D1%81%D0%BB%D0%B5%D0%BD%D0%BD%D1%8F.

10. What is Cloud Security? How to secure Cloud [Електронний ресурс] – Режим доступу: https://www.skyhighsecurity.com/en-us/cybersecurity-defined/what-is-cloud-security.html.

11. Top 12 Cloud Security Best Practives [2022] [Електронний ресурс] – Режим доступу: https://www.esecurityplanet.com/cloud/cloud-security-best-practices/.

12. A Step-by-Step Guide to Cloud Security Best Practives [Електронний ресурс] – Режим доступу: https://readwrite.com/secure-platform-as-a-service/.

13. A Comprehensive Guide to Cloud Security in 2022 [Електронний ресурс] – Режим доступу: https://kinsta.com/blog/cloud-security/

14. Top 12 Cloud Security Tools for 2022 [Електронний ресурс] – Режим доступу: https://spectralops.io/blog/top-12-cloud-security-tools/

15. Everything You Need To Know About API Security [Електронний ресурс] – Режим доступу: https://www.cdnetworks.com/cloud-security-blog/api-security/

16. What is Data Loss Prevention in Cloud Computing [Електронний ресурс] – Режим доступу: https://www.teramind.co/blog/cloud-dlp/

17. What is Cloud Backup and How Doest it Work? [Електронний ресурс] – Режим доступу: https://www.techtarget.com/searchdatabackup/definition/cloud-backup

18. What Is Cloud Encryption? Benefits, Challenges & More [Електронний ресурс] – Режим доступу: https://www.crowdstrike.com/cybersecurity-101/cloud-security/cloud-encryption/

19. What is a CASB? Cloud Access Security Broker [Електронний ресурс] – Режим доступу: https://www.skyhighsecurity.com/en-us/cybersecurity-defined/what-is-a-casb.html

20. How User Behavior Analytics (UBA) can Improve Cloud Security [Електронний ресурс] – Режим доступу: https://www.lepide.com/blog/how-user-behavior-analytics-uba-can-improve-cloud-security/

21. Cloud-based malware is on the rise. How can you secure your business? [Електронний ресурс] – Режим доступу: https://www.malwarebytes.com/blog/business/2022/07/cloud-based-malware-is-on-the-rise-how-can-you-secure-your-business

22. What Is Cloud Security Monitoring? A Complete Guide [Електронний ресурс] – Режим доступу: https://www.blumira.com/glossary/cloud-security-monitoring/

23. Introduction to Cloud Asset Inventory [Електронний ресурс] – Режим доступу: https://cloud.google.com/asset-inventory/docs/overview

24. Overview of Web Security Scanner [Електронний ресурс] – Режим доступу: https://cloud.google.com/security-command-center/docs/concepts-web-security-scanner-overview

25. Identity-Aware Proxy overview [Електронний ресурс] – Режим доступу: https://cloud.google.com/iap/docs/concepts-overview

26. Cloud Data Loss Prevention [Електронний ресурс] – Режим доступу: https://cloud.google.com/dlp

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ
(ПРЕЗЕНТАЦІЯ)