МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ТЕХНОЛОГІЇ КОНТРОЛЮ ВІДПОВІДНОСТІ КОНФІГУРАЦІЙ ХМАРНИХ ІНФРАСТРУКТУР СТАНДАРТАМ БЕЗПЕКИ”

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека
освітньо-професійної програми Управління інформаційною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ Артем КОРОВАЙЧЕНКО

(Підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ-61
Артем КОРОВАЙЧЕНКО

Керівник
к.т.н.: Дмитро РАБЧУН

Рецензент
д.т.н., професор: Галина ГАЙДУР

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Захисту інформації

Кафедра Управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти магістр

Спеціальність 125 Кібербезпека
Освітньо-професійна програма Управління інформаційною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедрою УІКБ
_____ Світлана ЛЕГОМІНОВА
“___”_____2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Коровайченку Артему Юрійовичу

(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи: “Технології контролю відповідності конфігурацій хмарних інфраструктур стандартам безпеки”
керівник кваліфікаційної роботи Дмитро РАБЧУН, к.т.н.
(Ім’я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “19“ жовтня 2023 р. №145
2. Строк подання кваліфікаційної роботи “18” грудня 2023 р.
3. Вихідні дані до кваліфікаційної роботи: *безпека хмарних інфраструктур*, *технології контролю конфігурації безпеки*, *нормативні документи, стандарти, міжнародні стандарти.*
4. Перелік питань, які потрібно розробити:
    1. Аналіз сутності хмарних середовищ та способи їх застосування.
    2. Огляд актуальних загроз та методів захисту хмарних середовищ.
    3. Шляхи застосування технологій контролю відповідності хмарних конфігурацій стандартам інформаційної безпеки.
5. Перелік ілюстративного матеріалу: *презентація*.
6. Дата видачі завдання “02” жовтня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання: “02” жовтня 2023 р.

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	12.10.2023	виконано
2.	Збір та аналіз літератури.	17.10.2023	виконано
3.	Аналіз хмарних інфраструктур, їх видів та складових.	20.10.2023	виконано
4.	Дослідження методів захисту хмарних інфраструктур.	25.10.2023	виконано
5.	Аналіз актуальних загроз безпеці хмарних інфраструктур.	30.10.2023	виконано
6.	Розробка методів застосування технологій контролю відповідності хмарних конфігурацій стандартам.	08.11.2023	виконано
7.	Формулювання висновків за результатами проведеного дослідження.	20.11.2023	виконано
8.	Оформлення роботи.	02.12.2023	виконано
9.	Оформлення презентації.	05.12.2023	виконано
10.	Отримання рецензії на роботу.	18.12.2023	виконано
11.	Захист в ДЕК.	16.01.2024	виконано

Здобувач вищої освіти _____ Артем КОРОВАЙЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Дмитро РАБЧУН
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Коровайченко А.Ю. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною безпекою
(назва)
на тему: "Технології контролю відповідності конфігурацій хмарних інфраструктур стандартам безпеки"
Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Віталій САВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач **КОРОВАЙЧЕНКО Артем** у кваліфікаційній роботі дослідив поняття хмарних інфраструктур, їх видів та складових, дослідив актуальні загрози таким середовищам та методи захисту, розробив шляхи застосування технологій контролю відповідності конфігурацій хмарних інфраструктур стандартам безпеки. **КОРОВАЙЧЕНКО Артем** показав розуміння проблеми дослідження та бачення основних теоретичних та практичних напрямів її вирішення, довів уміння самостійного застосування методів наукового дослідження, проявив себе як організований, відповідальний виконавець.

Це дозволяє оцінити виконану кваліфікаційну роботу здобувачу **КОРОВАЙЧЕНКУ Артему** на оцінку "відмінно" та присвоїти йому кваліфікацію "Магістр кібербезпеки за освітньо-професійною програмою "Управління інформаційною безпекою".

Керівник кваліфікаційної роботи _____ Дмитро РАБЧУН
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____"_____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Коровайченко А.Ю. допускається до захисту даної роботи в Державній екзаменаційній комісії.

Завідувач кафедри
Управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну магістерську роботу

Здобувач вищої освіти Коровайченко Артем Юрійович

на тему “Технології контролю відповідності конфігурацій хмарних інфраструктур стандартам безпеки”

Актуальність. У сучасному взаємопов’язаному цифровому світі хмарні обчислення стали основою бізнес-операцій, пропонуючи гнучкість, масштабованість і економічну ефективність. Однак із поширенням хмарних сервісів організації тепер стикаються з безпрецедентними проблемами щодо забезпечення безпеки та відповідності своїх цифрових активів. Управління безпекою в хмарі стало життєво важливою дисципліною в цьому середовищі, що дозволяє організаціям оцінювати, контролювати та підтримувати рівень безпеки у своїх хмарних середовищах. З метою захисту конфіденційних даних та зменшення ризиків, контроль відповідності конфігурацій став важливою складовою стратегії кібербезпеки хмарних інфраструктур.

Позитивні сторони

1. Дослідження, проведені в роботі, допомагають визначити та розробити найкращі практики впровадження технологій контролю відповідності конфігурацій безпеки хмарних середовищ стандартам. Організації можуть використовувати їх для підвищення рівня безпеки, зменшення вразливості та пом’якшення потенційних ризиків.
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки.

Недоліки

1. Доцільно було б описати інші інструменти та методи захисту хмарних інфраструктур для кращого розуміння спектру можливостей розробки заходів безпеки.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує позитивної оцінки, а здобувач Коровайченко Артем Юрійович заслуговує присвоєння кваліфікації “Магістр кібербезпеки” за освітньо-професійною програмою “Управління інформаційною безпекою”.

Рецензент:
Завідувач кафедри
Інформаційної
та кібернетичної безпеки,
д.т.н., професор _____ Галина ГАЙДУР
(підпис)

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 85 стор., 8 рис., 0 табл., 61 джерел.

Метою роботи є огляд хмарних середовищ, їх типів та методів захисту від наявних загроз, а також розробка шляхів імплементації інструментів контролю відповідності безпекових конфігурацій відповідно до стандартів безпеки та регуляторних норм.

Об'єктом дослідження є безпека хмарних інфраструктур та відповідність їх конфігурацій стандартам безпеки.

Предмет дослідження - інструменти безпеки, які використовуються у хмарних середовищах, дозволяючи тримати стан захищеності систем у відповідності до стандартів та регуляторних норм.

Методи дослідження. Було проведено збір і аналіз наявної літератури, наукових робіт, статей і галузевих звітів про інструменти CSPM. Аналізуючи детальні інтерв'ю з ключовими відділами в компаніях, такими як групи безпеки, адміністратори хмарних середовищ, було зібрано проблеми та перспективи, пов'язані з впровадженням інструментів CSPM. Також проведено порівняльний аналіз для оцінки сильних та слабких сторін цих інструментів.

Короткий зміст роботи. У роботі було проаналізовано ландшафт інструментів CSPM, їх функції та переваги. Були розглянуті ключові можливості, такі як автоматизована оцінка ризиків, моніторинг у реальному часі та застосування політик безпеки. Досліджено різноманітні хмарні платформи та сервіси, які підтримуються інструментами CSPM, включаючи таких основних постачальників, як Amazon Web Services (AWS), Microsoft Azure та Google Cloud Platform (GCP).

Галузь застосування цього дослідження поширюється на будь-яку організацію, яка використовує хмарні сервіси та прагне підвищити рівень безпеки в хмарі шляхом ефективного впровадження інструментів CSPM та керування ними.

КЛЮЧОВІ СЛОВА: ІНФОРМАЦІЙНА БЕЗПЕКА, ХМАРНІ ІНФРАСТРУКТУРИ, ТЕХНОЛОГІЇ КОНТРОЛЮ, СТАНДАРТИ.

ABSTRACT

The text part of the qualification work for the master's degree: 81 pages, 8 figures, 0 tables, 61 sources.

The purpose of the work is an overview of cloud environments, their types and methods of protection against existing threats, as well as the development of ways of implementing tools for monitoring the compliance of security configurations in accordance with security standards and regulatory norms.

Object of research is the security of cloud infrastructures and compliance of their configurations with security standards.

Subject of research is security tools used in cloud environments, allowing to keep the state of security of systems in accordance with standards and regulatory norms.

Research methods. A collection and analysis of available literature, research papers, articles, and industry reports on CSPM tools was conducted. Analyzing in-depth interviews with key departments in companies, such as security teams, cloud administrators, and business units, challenges and perspectives related to the implementation of CSPM tools were collected. A comparative analysis was also conducted to assess the strengths and weaknesses of these tools.

Brief content of research. The paper analyzed the landscape of CSPM tools, studying their functions and advantages. Key capabilities offered by these tools, such as automated risk assessment, real-time monitoring, and enforcement of security policies, were reviewed. Various cloud platforms and services supported by CSPM tools are explored, including major providers such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

Field of research extends to any organization that uses cloud services and seeks to improve cloud security by effectively implementing and managing CSPM tools.

KEYWORDS: INFORMATION SECURITY, CLOUD INFRASTRUCTURES, CONTROL TECHNOLOGIES, STANDARDS.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

CSPM	–	Cloud Security Posture Management, управління безпекою в хмарі
GDPR	–	General Data Protection Regulation, загальний регламент захисту даних
NIST	–	National Institute of Standards and Technology, національний інститут стандартів і технологій
HIPAA	–	Health Insurance Portability and Accountability Act, закон про перенесення та підзвітність медичного страхування
IaaS	–	Infrastructure as a Service, інфраструктура як послуга
SaaS	–	Software as a Service, програмне забезпечення як послуга
PaaS	–	Platform as a Service, платформа як послуга
DLP	–	Data Loss Prevention, запобігання втраті даних
DDoS	–	Distributed Denial-of-Service, розподілена відмова в обслуговуванні
APT	–	Advanced Persistent Threat, розширена постійна загроза
ACL	–	Access Control List, список контролю доступу
API	–	Application Programming Interface, інтерфейс прикладного програмування
ПЗ	–	Програмне забезпечення
CI/CD	–	Continuous Integration/Continuous Delivery, безперервна інтеграція та безперервна доставка
IaC	–	Infrastructure as Code, інфраструктура як код
IAM	–	Identity and Access Management, керування ідентифікацією та доступом
CSP	–	Cloud Service Provider, постачальник хмарних послуг

ВСТУП

Актуальність теми. Хмарні обчислення революціонізували спосіб роботи компаній, надаючи масштабовані та гнучкі рішення для зберігання даних, обчислень і програмних послуг. Однак широке впровадження хмарних технологій також породило нові виклики та ризики, особливо у сфері безпеки.

Безпека хмарних середовищ стала серйозною проблемою для організацій, оскільки конфіденційні дані та критично важлива інфраструктура переміщуються у зовнішнє хмарне середовище. Динамічний характер хмарних обчислень із його спільними ресурсами та розподіленою архітектурою створює унікальні аспекти безпеки, які відрізняються від традиційних локальних систем.

Ця робота має на меті глибше заглибитися у сферу хмарної безпеки, досліджуючи поточний ландшафт загроз, ключові вразливості та потенційні виклики, з якими стикаються організації, що використовують хмарні сервіси.

Інструменти Cloud Security Posture Management (CSPM) стали критично важливим рішенням для розв’язання цих проблем. Вони пропонують організаціям комплексний підхід до керування й оцінки рівня безпеки в хмарі, дозволяючи їм виявляти неправильні конфігурації, вразливості та забезпечувати відповідність галузевим і нормативним стандартам.

У роботі було проаналізовано ландшафт інструментів CSPM, вивчаючи їхні функції та переваги. Були розглянуті ключові можливості, які пропонують ці інструменти, такі як автоматизована оцінка ризиків, моніторинг у реальному часі та застосування політик безпеки. Досліджено різноманітні хмарні платформи та сервіси, які підтримуються інструментами CSPM, включаючи таких основних постачальників, як Amazon Web Services (AWS), Microsoft Azure та Google Cloud Platform (GCP).

Використовуючи інструменти CSPM, організації можуть отримати кращу видимість і контроль над своїм становищем безпеки в хмарі, проактивно виявляти ризики та вразливі місця та ефективно усувати будь-які проблеми. Це дослідження надає цінну інформацію та рекомендації для організацій, які прагнуть покращити керування безпекою в хмарі, дозволяючи їм безпечно

використовувати переваги хмарних обчислень, одночасно зменшуючи потенційні ризики та забезпечуючи відповідність.

Мета роботи. Дослідження спрямоване на те, щоб зрозуміти існуючі інструменти CSPM, доступні на ринку, і оцінити їхні можливості, функції та складність впровадження. Це включає в себе аналіз таких факторів, як простота використання, масштабованість, можливості інтеграції та загальна ефективність забезпечення безпеки хмари. Роботу також зосереджено на оцінці інструментів, які можуть допомогти компаніям виконувати вимоги відповідності, такі як GDPR, NIST 800-53 або галузеві норми. Також включено перевірку того, чи пропонують інструменти такі функції, як автоматичні перевірки відповідності та механізми звітування.

Об'єкт дослідження - підвищення рівня безпеки компаній у хмарі, захист їх цифрових активів, пом'якшення ризиків та відповідність вимогам стандартів.

Предмет дослідження - різноманітні інструменти CSPM, доступні на ринку та порівняння їх основних функцій, можливостей, ефективності та придатності для потреб хмарної безпеки організацій.

Для досягнення цієї мети в роботі необхідно виконати наступні *завдання:*

1. Дослідити і визначити доступні інструменти CSPM на ринку.
2. Оцінити їхні функції, можливості, параметри розгортання, масштабованість та підтримку.

Методи дослідження. Було проведено збір і аналіз наявної літератури, наукових робіт, статей і галузевих звітів про інструменти CSPM. Аналізуючи детальні інтерв'ю з ключовими відділами в компаніях, такими як групи безпеки, адміністратори хмарних середовищ та бізнес-підрозділи, було зібрано проблеми та перспективи, пов'язані з впровадженням інструментів CSPM. Також проведено порівняльний аналіз для оцінки сильних та слабких сторін цих інструментів. Це передбачає порівняння їхніх функцій, можливостей, моделей розгортання, інтеграції, цін і відгуків клієнтів.

Наукова новизна одержаних результатів. Робота може сприяти прогресу в області інструментів CSPM. Оцінюючи різні інструменти, виявляючи їхні

сильні та слабкі сторони, а також визначаючи прогалини або області для вдосконалення, дослідження може надати цінний зворотній зв’язок постачальникам інструментів і сприяти розвитку та інноваціям інструментів CSPM.

Практичне значення одержаних результатів. Дослідження інструментів CSPM є актуальними в сучасному технологічному середовищі, де зростає впровадження хмарних технологій, а компанії стикаються з різними загрозами безпеці та проблемами відповідності. Вирішуючи їх, дослідження сприяє отриманню знань, які можна застосувати в процесі підвищення рівня захищеності компаній.

Галузь застосування цього дослідження поширюється на будь-яку організацію, яка використовує хмарні сервіси та прагне підвищити рівень безпеки в хмарі шляхом ефективного впровадження інструментів CSPM та керування ними.

РОЗДІЛ 1
СУТНІСТЬ ХМАРНИХ СЕРЕДОВИЩ ТА СПОСОБИ ЇХ ЗАСТОСУВАННЯ

1.1. Що таке хмарне середовище?

Розробка та побудова обчислювальної інфраструктури може коштувати багато часу та грошей. Підприємствам необхідно купувати фізичні сервери та інше обладнання через закупівельні процеси, які можуть тривати місяцями, а в подальшому підтримувати та обслуговувати такі центри. Придбані системи вимагають фізичного простору, як правило, спеціалізованого приміщення з достатньою потужністю та охолодженням. Після налаштування та розгортання таких комплексів підприємствам потрібен експертний персонал для керування ними [26].

Таку інфраструктуру важко масштабувати, коли зростає попит або бізнес розширюється. Підприємства можуть придбати більше обчислювальних ресурсів, ніж потрібно, що призведе до низького рівня використання.

Хмарні середовища вирішують ці проблеми, пропонуючи обчислювальні ресурси як масштабовані послуги на вимогу. Загалом це сервери, сховища, бази даних, мережі, програмне забезпечення, за які потрібно платити лише коли ними користуються. Це допомагає знизити операційні витрати, ефективніше керувати інфраструктурою та масштабувати її відповідно до потреб бізнесу.

Моделі послуг хмарних обчислень базуються на концепції спільного використання обчислювальних ресурсів, програмного забезпечення та інформації на вимогу через Інтернет. Компанії або окремі особи платять за доступ до віртуального пулу спільних ресурсів, включаючи обчислювальні, сховища та мережеві послуги, які розташовані на віддалених серверах, якими володіють і керують постачальники послуг.

«Хмари» використовують мережу для підключення користувачів до хмарної платформи, де вони запитують і отримують доступ до орендованих

обчислювальних послуг. Центральний сервер обробляє весь зв’язок між клієнтськими пристроями та серверами для полегшення обміну даними. Функції безпеки та конфіденційності є звичайними компонентами для збереження цієї інформації.

При застосуванні архітектури хмарних обчислень не існує універсального рішення для всіх. Те, що працює для іншої компанії, може не відповідати вам і потребам вашого бізнесу. Насправді ця гнучкість і універсальність є однією з характерних рис хмари, що дозволяє підприємствам швидко адаптуватися до змін ринків або показників.

1.2. Сервіс-моделі хмарних середовищ

Хмарні обчислення дають розробникам та IT-відділам можливість зосередитися на найважливішому та уникнути недиференційованої роботи, як-от закупівлі, технічне обслуговування та планування потужностей. Зі зростанням популярності таких послуг з’явилося кілька різних моделей їх надання, які допомагають задовольнити конкретні потреби різних користувачів. Кожен тип хмарної служби та метод розгортання надає різні рівні контролю, гнучкості та керування. Розуміння відмінностей між інфраструктурою як послугою, платформою як послугою та програмним забезпеченням як послугою, а також те, які стратегії розгортання можна використовувати, допоможе вирішити, який набір послуг підходить для конкретних потреб [27].

Розрізняють три основні моделі надання послуг хмарних обчислень.

Інфраструктура як послуга (IaaS)

Інфраструктура як послуга (рис. 1.1.), іноді скорочена як IaaS, містить основні складові компоненти обчислювальних систем і зазвичай забезпечує доступ до мережевих функцій, комп’ютерів (віртуальних або на спеціальному апаратному забезпеченні) і простору для зберігання даних. Така модель надає найвищий рівень гнучкості та контролю над вашими IT-ресурсами та найбільш

схожа на існуючі IT-ресурси, з якими сьогодні знайомі багато IT-відділів і розробників.

Інфраструктура як послуга дозволяє легке перенесення програмного забезпечення або робочого навантаження в хмару. Без рефакторингу базової архітектури можна збільшити масштаб і продуктивність, посилити безпеку та зменшити витрати на виконання програми або процесинг робочого навантаження.

Завдяки такій системі розробники мають можливість швидко налаштувати та демонтувати середовища тестування та розробки, швидше виводячи нові програми на ринок. IaaS дозволяє швидко та економно масштабувати середовища розробки/тестування вгору та вниз.

Компанії можуть уникати капітальних витрат на зберігання даних та складності керування сховищами, що зазвичай потребує кваліфікованого персоналу та дотримання вимог законодавства та відповідності. IaaS корисний для обробки непередбачуваного попиту та постійно зростаючих потреб у сховищі. Разом із цим спрощується планування та керування системами резервного копіювання та відновлення [28].

Така модель надає всю інфраструктуру для підтримки веб-додатків, включаючи сховище та веб-сервер, а також мережеві ресурси. Організація може швидко розгортати веб-програми на IaaS і легко масштабувати інфраструктуру, коли попит на програми непередбачуваний.

Високопродуктивні обчислення на суперкомп’ютерах, комп’ютерних мережах або комп’ютерних кластерах допомагають вирішувати складні проблеми, що включають мільйони змінних та велику кількість обчислень [1].

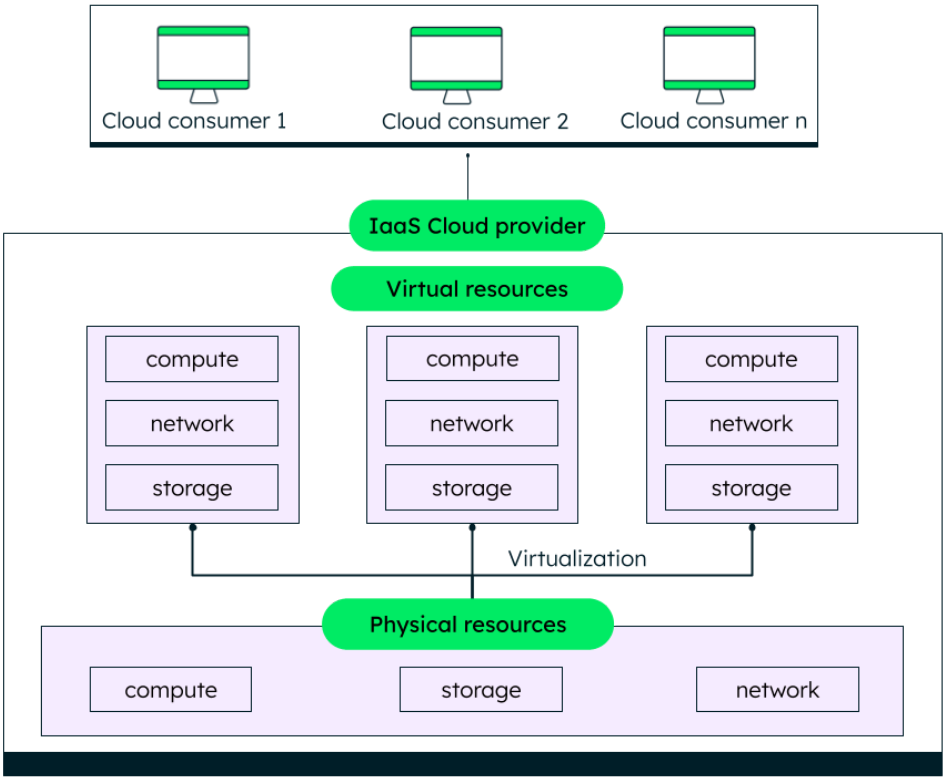

Рис. 1.1. Інфраструктура як послуга [2]

Платформа як послуга (PaaS)

Платформа як послуга (рис. 1.2.) позбавляє організації від необхідності керувати основною інфраструктурою (зазвичай апаратним забезпеченням і операційними системами) і дозволяють зосередитися на розгортанні та управлінні програмами. Це допомагає бути ефективнішим, оскільки не потрібно турбуватися про закупівлю ресурсів, планування потужностей, технічне обслуговування програмного забезпечення, встановлення виправлень або будь-яку іншу недиференційовану діяльність, пов’язану з роботою вашої програми.

У моделі PaaS усе керування бекендом здійснюється через інфраструктуру постачальника. Це означає, що підприємствам не потрібно встановлювати громіздкі інструменти розробника на локальні комп’ютери або керувати складними контейнерними оркестраторами, такими як Kubernetes. Натомість продукти PaaS надаються через Інтернет, що робить їх доступнішими та простішими у використанні.

Платформа як послуга надає інструменти розробки через онлайн-інтерфейс. Це означає, що замість того, щоб мати можливість працювати лише з локального комп'ютера, розробники програмного забезпечення можуть входити з будь-якого місця, забезпечуючи більшу гнучкість для розосереджених і віддалених команд. За допомогою PaaS розробники мають доступ до програмного та апаратного забезпечення, необхідного для розробки, тестування та обслуговування додатків.

Важливо відзначити, що PaaS не повністю замінює IT-інфраструктуру компанії. Натомість він використовує постачальника хмарних послуг, щоб надати користувачам доступ до середовища виконання для розробки програм через веб-браузер. Пропозиції PaaS можна надавати через різні типи хмар, як-от загальнодоступні, приватні та гібридні, для надання різних послуг, таких як розміщення додатків, розробка Java тощо [29].

Крім простору для розробки, PaaS може містити керовані та масштабовані хмарні бази даних, підтримку різних мов, мобільні SDK і доступ до бібліотеки. Усе це робить його ефективною та доступною альтернативою налагодженню, експлуатації та підтримці внутрішнього середовища, розміщеного на локальних IT-службах.

Організації зазвичай використовують PaaS для наступних сценаріїв:

Фреймворк для розробки. PaaS надає структуру, на основі якої розробники можуть розробляти або налаштовувати програмне забезпечення на основі хмарних середовищ. Подібно до того, створюються макроси в Excel, PaaS дозволяє розробникам створювати програми за допомогою вбудованих програмних компонентів, включаючи такі функції, як масштабованість, висока доступність і можливість роботи з кількома клієнтами, що зменшує кількість роботи, яку мають виконувати розробники.

Аналітика. Інструменти, які надаються з PaaS, дозволяють організаціям аналізувати та добувати їх дані, знаходити інформацію та закономірності, прогнозувати результати покращень після зміни дизайну продукту, повернення інвестицій та інших бізнес-рішень [1].

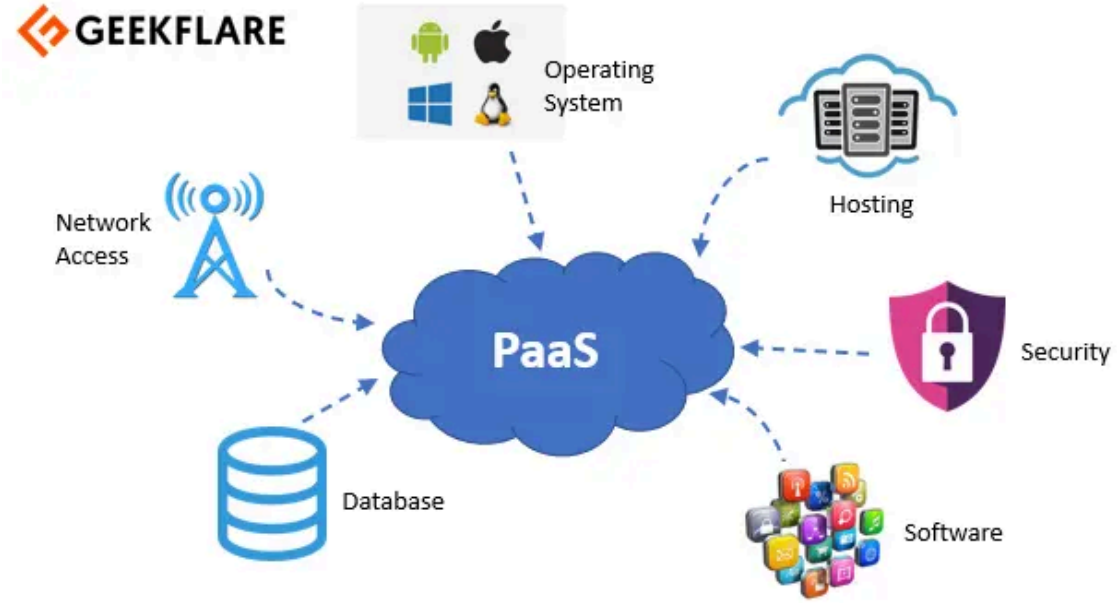

Рис. 1.2. Платформа як послуга [3]

Програмне забезпечення як послуга (SaaS)

Програмне забезпечення як послуга (рис. 1.3.) надає готовий продукт, який працює та керується постачальником послуг. У більшості випадків люди, які говорять про програмне забезпечення як послугу, мають на увазі програми для кінцевих користувачів. З пропозицією SaaS немає потреби думати про те, як підтримується служба або як керується базовою інфраструктурою; вам потрібно лише подумати про те, як ви будете використовувати цю конкретну частину програмного забезпечення. Типовим прикладом програми SaaS є веб-електронна пошта, де ви можете надсилати й отримувати електронну пошту без необхідності керувати доповненнями функцій до продукту електронної пошти чи підтримувати сервери й операційні системи, на яких працює програма електронної пошти.

SaaS надає повне програмне рішення, яке можна купити на основі оплати за використання у постачальника хмарних послуг. Компанії орендують програму, а користувачі мають змогу підключатися до неї через Інтернет, зазвичай за допомогою веб-браузера. Уся основна інфраструктура, програмне забезпечення та дані програм розташовані в центрі обробки даних постачальника послуг. Він керує апаратним і програмним забезпеченням і за

допомогою відповідної угоди про надання послуг забезпечує доступність і безпеку програми та ваших даних. SaaS дозволяє організаціям швидко налагодити роботу за допомогою програми за мінімальних початкових витрат.

Рис. 1.3. Програмне забезпечення як послуга [4]

1.3. Переваги використання хмарних середовищ

Послуги хмарних обчислень існують приблизно два десятиліття, і, незважаючи на дані, що вказують на ефективність бізнесу, економічні вигоди та конкурентні переваги, які вони мають, значна частина бізнес-спільноти продовжує працювати без них. Згідно з дослідженням International Data Group [30], 69% підприємств уже використовують хмарні технології в тій чи іншій якості, а 18% кажуть, що планують у певний момент запровадити рішення для хмарних обчислень. У той же час Dell повідомляє, що компанії, які інвестують у великі дані, хмару, мобільність і безпеку, мають на 53% швидше зростання прибутку, ніж їхні конкуренти. Як показують ці дані, все більше технічно підкованих компаній і лідерів галузі визнають численні переваги тенденції хмарних обчислень. Але більше того, вони використовують цю технологію, щоб

ефективніше керувати своїми організаціями, краще обслуговувати клієнтів і значно підвищити загальну норму прибутку [5].

Хмарні обчислення – це термін, який набув широкого поширення за останні кілька років. З експоненційним зростанням використання даних, яке супроводжує перехід суспільства в цифрове 21 століття, окремим особам і організаціям стає все важче підтримувати всю свою життєво важливу інформацію, програми та системи в робочому стані на внутрішніх комп'ютерних серверах. Рішення цієї проблеми існує майже стільки ж, скільки і Інтернет, але воно лише нещодавно набуло широкого застосування в бізнесі.

Хмарні обчислення працюють за принципом, подібним до веб-клієнтів електронної пошти, дозволяючи користувачам отримувати доступ до всіх функцій і файлів системи без необхідності зберігати основну частину цієї системи на своїх комп'ютерах. Насправді більшість людей вже користуються різними службами хмарних обчислень, навіть не підозрюючи про це. Gmail, Google Drive, TurboTax і навіть Facebook та Instagram — це хмарні програми. Для всіх цих послуг користувачі надсилають свої особисті дані на хмарний сервер, який зберігає інформацію для подальшого доступу. І якими б корисними ці програми не були для особистого користування, вони ще більш цінні для компаній, яким потрібен доступ до великих обсягів даних через захищене онлайн-з'єднання.

Тим не менш, є лідери, які все ще вагаються щодо рішень із застосуванням хмарних обчислень для своїх організацій. Тому, нижче будуть наведені переваги, які можуть спонукати такі компанії інтегрувати «хмару» в їх процеси.

Економія. 20% організацій стурбовані початковою вартістю впровадження хмарного середовища. Але ті, хто намагається зважити переваги та недоліки використання хмари, повинні враховувати більше факторів, ніж лише початкову ціну, вони повинні враховувати рентабельність інвестицій.

Перебуваючи в хмарі, легкий доступ до даних компанії заощадить час і гроші на запуск проєктів. А для тих, хто хвилюється, що в кінцевому підсумку

їм доведеться платити за функції, які їм не потрібні, більшість хмарних обчислювальних сервісів оплачуються по мірі використання. Це означає, що якщо ви не скористаєтеся певними функціями хмари, то принаймні не доведеться витрачати на них гроші.

Система оплати за використанням також поширюється на простір для зберігання даних, необхідний для обслуговування зацікавлених сторін і клієнтів, що означає, що організації отримають рівно стільки місця, скільки їм потрібно, і не стягуватиметься плата за простір, який не використовується. У сукупності ці фактори призводять до зниження витрат і підвищення прибутку. Половина всіх IT-директорів та IT-лідерів, опитаних Bitglass, повідомили про економію коштів у 2015 році в результаті використання хмарних рішень.

Гнучкість. Бізнес має лише обмежену кількість фокусів, які потрібно розподілити між усіма його обов'язками. Якщо поточні рішення змушують приділяти занадто багато уваги питанням обладнання та зберігання даних, не буде змоги зосередитися на досягненні бізнес-цілей і задоволенні клієнтів. З іншого боку, покладаючись на зовнішню організацію, яка опікуватиметься всім IT-хостингом та інфраструктурою, компанії матимуть більше часу, який можна присвятити аспектам бізнесу, які безпосередньо впливають на прибуток [31].

Хмара пропонує компаніям більшу гнучкість у порівнянні з розміщенням на локальному сервері. І якщо потрібна додаткова пропускна здатність, сервіс може миттєво задовольнити цю вимогу, замість того, щоб піддаватися складному (і дорогому) оновленню IT-інфраструктури. Ця покращена свобода та гнучкість може істотно змінити загальну ефективність організації. Більшість 65% респондентів опитування InformationWeek сказали, що «здатність швидко задовольняти бізнес-вимоги» була однією з найважливіших причин переходу бізнесу в хмарне середовище.

Мобільність. Хмарні обчислення забезпечують зручний доступ до корпоративних даних за допомогою смартфонів і пристроїв, що є чудовим способом гарантувати, що ніхто ніколи не залишиться осторонь. Співробітники з напруженим графіком або ті, хто живе далеко від корпоративного офісу,

можуть використовувати цю функцію, щоб миттєво бути в курсі подій з клієнтами та колегами.

Через хмару можна пропонувати зручно доступну інформацію торговому персоналу, який подорожує, позаштатним працівникам або віддаленим співробітникам, щоб покращити баланс між роботою та особистим життям. Тому не дивно бачити, що організації, для яких задоволеність співробітників є пріоритетом, мають на 24% більше шансів розширити використання хмари.

Аналітика. У міру просування в епоху цифрових технологій стає дедалі ясніше, що стара приказка «Знання — це сила» набула сучаснішої та точнішої форми: «Дані — це гроші». У мільйонах бітів даних, які оточують ваші клієнтські транзакції та бізнес-процеси, сховані шматки безцінної інформації, що діє, і чекає, щоб їх ідентифікували та вжили заходів. Звичайно, просіяти ці дані, щоб знайти ядра, може бути дуже важко, якщо немає доступу до правильного рішення хмарних обчислень [32].

Багато хмарних рішень для зберігання пропонують інтегровану хмарну аналітику для перегляду даних з висоти пташиного польоту. З інформацією, що зберігається в хмарі, можна легко запровадити механізми відстеження та створювати індивідуальні звіти для аналізу інформації в масштабах організації. Завдяки цій інформації можна підвищити ефективність і розробити плани дій для досягнення цілей організації. Наприклад, компанія з виробництва напоїв Sunny Delight змогла збільшити прибуток приблизно на 2 мільйони доларів на рік і скоротити витрати на персонал на 195 000 доларів завдяки хмарній бізнес-аналітиці.

Покращена співпраця. Якщо в компанії є два чи більше співробітників, то співпраця має бути головним пріоритетом. Зрештою, немає сенсу мати команду, якщо вона не може працювати як команда. Хмарні обчислення роблять процес співпраці простим. Члени команди можуть легко та безпечно переглядати інформацію та обмінюватися нею на хмарній платформі. Деякі хмарні служби навіть надають спільні соціальні простори для об’єднання співробітників у вашій організації, таким чином підвищуючи інтерес і залученість. Співпраця

може бути можливою без рішення хмарних обчислень, але вона ніколи не буде такою легкою та ефективною.

Контроль якості. Є кілька речей, які так згубно впливають на успіх бізнесу, як низька якість і непослідовна звітність. У хмарній системі всі документи зберігаються в одному місці та в єдиному форматі. Завдяки тому, що всі мають доступ до однієї інформації, є змога підтримувати узгодженість даних, уникати людських помилок і мати чіткий запис про будь-які перегляди чи оновлення. І навпаки, керування інформацією в розрізненому вигляді може призвести до того, що працівники випадково збережуть різні версії документів, що призведе до плутанини та розрідження даних.

Відновлення після аварії. Одним із факторів, що сприяє успіху бізнесу, є контроль. На жаль, незалежно від того, наскільки організація може контролювати свої власні процеси, завжди будуть речі, які повністю виходять з-під контролю, і на сучасному ринку навіть невелика кількість непродуктивних простоїв може мати різко негативний ефект. Перерви у роботі послуг призводять до втрати продуктивності, прибутку та репутації бренду. Хоча немає способу запобігти або навіть передбачити катастрофи, які потенційно можуть зашкодити організації, можна зробити дещо, щоб пришвидшити відновлення. Хмарні служби забезпечують швидке відновлення даних у будь-яких надзвичайних ситуаціях, від стихійних лих до відключень електроенергії. У той час як 20% користувачів хмари стверджують, що аварійне відновлення за чотири години або менше, лише 9% користувачів, які не використовують хмару, можуть стверджувати те саме. У нещодавньому опитуванні 43% IT-керівників заявили, що планують інвестувати або покращити хмарні рішення для аварійного відновлення.

Запобігання втратам. Якщо організація не інвестує в рішення для хмарних обчислень, тоді всі цінні дані нерозривно пов’язані з офісними комп’ютерами, на яких вони зберігаються. Це може не виглядати як проблема, але реальність така, що якщо виникне проблема з обладнанням, є ризик назавжди втратити дані. Це більш поширена проблема, ніж можна собі уявити.

Комп’ютери можуть не працювати з багатьох причин, починаючи від вірусного ПЗ і закінчуючи віковим погіршенням апаратного забезпечення та простою помилкою користувача. Або, незважаючи на найкращі наміри, їх можуть загубити або вкрасти (щотижня у великих аеропортах втрачається понад 10 000 ноутбуків).

Без використання хмарних рішень існує ризику втратити всю інформацію, яка зберігалася локально. Однак за допомогою хмарного сервера вся інформація залишається в безпеці та легкодоступна з будь-якого комп’ютера, підключеного до Інтернету.

Автоматичне оновлення програмного забезпечення. Хмарні програми оновлюються автоматично замість того, щоб змушувати ІТ-відділ виконувати оновлення вручну для всієї організації. Це економить дорогоцінний час і гроші ІТ-спеціалістів, витрачені на сторонні ІТ-консультації. PCWorld перераховує, що 50% тих, хто використовує хмарні рішення, назвали потребу в меншій кількості внутрішніх ІТ-ресурсів як перевагу хмари.

Безпека: Багато організацій мають проблеми з безпекою, коли мова заходить про впровадження хмарних рішень. Зрештою, коли файли, програми та інші дані не зберігаються надійно на місці неможливо знати, що вони захищені.

Постійна робота хмарного хоста полягає в тому, щоб ретельно стежити за безпекою, що є значно ефективнішим, ніж звичайна власна система, де організація повинна розподілити свої зусилля між безліччю проблем ІТ, причому безпека є лише однією з них. І хоча більшість компаній не люблять відкрито розглядати можливість внутрішньої крадіжки даних, правда полягає в тому, що приголомшливо високий відсоток компрометації даних відбувається всередині компанії і вчиняється працівниками. Коли це так, насправді набагато безпечніше зберігати конфіденційну інформацію поза офісом організації.

RapidScale стверджує [33], що 94% підприємств помітили покращення безпеки після переходу на хмару, а 91% сказали, що хмара полегшує відповідність державним вимогам. Ключем до цієї посиленої безпеки є шифрування даних, які передаються через мережі та зберігаються в базах

даних. Завдяки шифруванню інформація стає менш доступною для хакерів або тих, хто не має права переглядати ваші дані. Як додатковий захід безпеки для більшості хмарних служб можна встановити різні параметри безпеки залежно від користувача.

Висновки до першого розділу

Хмарні обчислення - це надання різних послуг через Інтернет. У розділі було детально розкрито поняття хмарних середовищ та їх складові. Ці ресурси включають такі інструменти та програми, як сховище даних, сервери, бази даних, мережі та програмне забезпечення. Завдяки аутсорсингу цих ресурсів компанії можуть отримати доступ до обчислювальних потужностей, які їм потрібні, коли вони їм потрібні, без необхідності купувати та підтримувати фізичну локальну IT-інфраструктуру. Це забезпечує гнучкість, швидші інновації та економію при масштабуванні. Для багатьох компаній хмарна міграція безпосередньо пов’язана з модернізацією даних та IT.

Хмарні середовища надають розширені обчислювальні ресурси, доступні на вимогу, які масштабуються за потреби, з регулярними оновленнями та без необхідності купувати та підтримувати локальну інфраструктуру. У розділі було описано існуючі моделі надання послуг хмарних обчислень, завдяки яким команди стають більш ефективними та скорочують час виходу на ринок, оскільки вони можуть швидко отримувати та масштабувати послуги без значних зусиль, які вимагають керування традиційною локальною інфраструктурою.

Хмарні обчислення зробили революцію в роботі компаній, запропонувавши неперевершені можливості для ефективності, співпраці та зростання. Усі їх переваги важко перерахувати, проте однією зі значних є можливість надавати клієнтам найвищий рівень обслуговування. У розділі було детально описано ключові переваги переходу компаній у хмарні середовища. Використовуючи хмару, компанії можуть збирати величезні обсяги даних, що

дозволяє їм отримати цінну інформацію про поведінку та вподобання клієнтів. Це, у свою чергу, забезпечує персоналізований та індивідуальний досвід клієнтів, підвищуючи задоволеність і лояльність.

РОЗДІЛ 2
БЕЗПЕКА ХМАРНИХ СЕРЕДОВИЩ

2.1. Важливість розробки заходів безпеки

Хмарна безпека – це набір процедур і технологій, призначених для боротьби із зовнішніми та внутрішніми загрозами безпеці бізнесу. Організаціям потрібне захищене середовище, коли вони рухаються до своєї стратегії цифрової трансформації та включають хмарні інструменти та служби як частину своєї інфраструктури [22].

Протягом останніх років терміни цифрова трансформація та хмарна міграція регулярно використовувалися в корпоративних налаштуваннях. Хоча обидві фрази можуть означати різні речі для різних організацій, кожна з них керується спільним знаменником: потребою в змінах.

Оскільки підприємства сприймають ці концепції та рухаються до оптимізації свого операційного підходу, виникають нові виклики під час балансування рівня продуктивності та безпеки. У той час як більш сучасні технології допомагають організаціям розширювати можливості поза межами локальної інфраструктури, перехід переважно до хмарних середовищ може мати кілька наслідків, якщо не буде здійснюватися безпечно.

Встановлення правильного балансу потребує розуміння того, як сучасні підприємства можуть отримати вигоду від використання взаємопов’язаних хмарних технологій із застосуванням найкращих практик хмарної безпеки.

У сучасних підприємствах спостерігається зростаючий перехід до хмарних середовищ і обчислювальних моделей IaaS, Paas або SaaS. Динамічний характер управління інфраструктурою, особливо при масштабуванні додатків і послуг, може спричинити низку проблем для підприємств при забезпеченні відповідними ресурсами своїх відділів. Ці моделі «як-послуги» надають організаціям можливість розвантажити багато трудомістких завдань, пов’язаних з IT [34].

Оскільки компанії продовжують мігрувати в хмару, розуміння вимог безпеки для збереження даних стає критичним. Хоча сторонні постачальники хмарних обчислень можуть взяти на себе керування цією інфраструктурою, відповідальність за безпеку активів даних і підзвітність не обов'язково переходить разом із цим.

За замовчуванням більшість хмарних провайдерів дотримуються найкращих практик безпеки та вживають активних заходів для захисту цілісності своїх серверів. Однак організаціям необхідно врахувати власні міркування, захищаючи дані, програми та робочі навантаження, що виконуються в хмарі.

Загрози безпеці стали більш розвиненими, оскільки цифровий ландшафт продовжує розвиватися. Ці загрози явно націлені на провайдерів хмарних обчислень через загальну відсутність видимості організації в доступі та переміщенні даних. Не вживаючи активних заходів для покращення безпеки своєї хмари, організації можуть зіткнутися зі значними ризиками управління та відповідності під час керування клієнтською інформацією, незалежно від того, де вона зберігається.

Хмарна безпека повинна бути важливою темою для обговорення незалежно від розміру підприємства. Хмарна інфраструктура підтримує майже всі аспекти сучасних обчислень у всіх галузях і в різних вертикалях.

Однак успішне впровадження хмарних технологій залежить від застосування відповідних заходів протидії для захисту від сучасних кібератак. Незалежно від того, чи працює організація в загальнодоступному, приватному чи гібридному хмарному середовищі, хмарні рішення безпеки та найкращі методи є необхідністю для забезпечення безперервності бізнесу.

Розробка заходів безпеки хмарного середовища має низку переваг. Насамперед, це краща видимість. Сильні методи захисту даних забезпечують їх безпеку та цілісність. Ці заходи включають надійну автентифікацію та контроль доступу, шифрування даних у стані спокою та передачі, регулярне резервне

копіювання та моніторинг будь-якого несанкціонованого доступу чи підозрілої активності.

Зберігаючи видимість внутрішньої роботи хмари, можна легко відстежувати та керувати даними. Компанії матимуть чітке уявлення про типи даних, які вони зберігають, де вони розташовані та хто має до них доступ. Ця видимість має вирішальне значення для дотримання правил захисту інформації та виявлення будь-яких потенційних ризиків безпеці.

Крім того, надійні заходи безпеки даних дозволяють відстежувати та контролювати дії користувачів у хмарному середовищі. Можна відстежувати, хто використовує хмарні служби, до яких даних вони мають доступ і як вони їх використовують. Цей рівень видимості допомагає виявляти будь-які спроби несанкціонованого доступу, виявляти потенційні порушення даних і швидко реагувати на будь-які інциденти безпеки [35].

Хмарні рішення для захисту даних не тільки забезпечують надійний захист інформації, але й пропонують широкий спектр додаткових функцій і переваг. Однією з таких є автоматизоване та стандартизоване резервне копіювання. Завдяки безпеці даних у хмарі можна налаштувати автоматичне резервне копіювання, забезпечуючи послідовний та регулярний процес без необхідності ручного втручання. Це звільняє команди від трудомісткого завдання моніторингу резервних копій і усунення будь-яких проблем, які можуть виникнути.

Хмарне аварійне відновлення є ще одним цінним аспектом безпеки хмарних даних. У разі аварії або втрати інформації хмарні рішення для аварійного відновлення дозволяють ефективно та швидко відновити стан інфраструктури. Це можна зробити за лічені хвилини, мінімізуючи будь-які потенційні простої та забезпечуючи безперервність бізнесу.

Хмарні рішення безпеки даних також часто включають такі функції, як шифрування даних, яке захищає конфіденційну інформацію, перетворюючи її на нечитабельний код, який можна розшифрувати лише за допомогою певного

ключа. Це додає додатковий рівень безпеки як у стані спокою, так і під час передачі.

Крім того, хмарні рішення безпеки даних часто пропонують можливості моніторингу та оповіщення в реальному часі. Це дозволяє бути в курсі будь-яких спроб несанкціонованого доступу, підозрілих дій або потенційних загроз безпеці. Отримавши негайні сповіщення, можна миттєво відреагувати на інциденти та вжити відповідних заходів для пом’якшення потенційної шкоди.

Методи захисту даних у хмарі забезпечують значну економію коштів за рахунок зниження загальної вартості володіння, пов’язаної з керуванням і захистом даних. Завдяки цьому організації можуть усунути потребу в локальній інфраструктурі, апаратному забезпеченні та витратах на обслуговування. Це призводить до зменшення капітальних і операційних витрат.

Крім того, такі рішення мінімізують адміністративне та управлінське навантаження, зазвичай пов’язане з традиційними заходами безпеки. Постачальники послуг хмарних обчислень виконують багато завдань, пов’язаних із безпекою даних, наприклад оновлення програмного забезпечення, налагодження та обслуговування системи. Це звільняє час і ресурси фахівців із безпеки, дозволяючи їм зосередитися на більш цінних видах діяльності та стратегічних ініціативах.

Однією з переваг використання хмарних середовищ є те, що постачальники пропонують найновіші функції та інструменти безпеки. Це означає, що спеціалісти з безпеки можуть використовувати найсучасніші технології та можливості для захисту своїх даних. Хмарні рішення безпеки часто включають автоматизацію, яка оптимізує процеси та добре інтегрується з існуючою інфраструктурою. Така опція не тільки зменшує ймовірність людської помилки, але й забезпечує швидший час реакції та покращує загальну безпеку.

Постійне сповіщення та моніторинг є ще однією ключовою перевагою безпеки хмарних даних. Хмарні рішення часто забезпечують моніторинг у реальному часі та оповіщення, які негайно сповіщають команди безпеки про виявлення потенційних загроз. Це дозволяє швидше реагувати на інциденти та

допомагає запобігти потенційним порушенням даних або несанкціонованому доступу.

На додаток до економії коштів і операційних переваг, надійні програми безпеки розроблені для виконання зобов'язань щодо відповідності стандартам та регламентам. Вимоги відрізняються залежно від галузі та географічного розташування, але зазвичай вони передбачають суворі правила щодо захисту даних, конфіденційності та безпеки.

Хмарні рішення безпеки даних можуть допомогти організаціям виконати ці зобов'язання, надаючи видимість того, де зберігаються дані, хто має до них доступ, як вони обробляються та як захищаються. Хмарні постачальники часто пропонують комплексні засоби контролю безпеки та надійні механізми шифрування для забезпечення конфіденційності, цілісності та доступності даних.

Запобігання втраті даних (DLP) є важливим компонентом комплексної програми захисту даних. Такі рішення допомагають організаціям легко виявляти, класифікувати та ідентифікувати конфіденційні дані, щоб зменшити ризик порушень. Це включає ідентифікацію та захист інформації, інтелектуальної власності, фінансових даних та іншої конфіденційної інформації, яку необхідно захистити [36].

Впроваджуючи хмарні рішення DLP, організації можуть застосовувати політику захисту даних і запобігати несанкціонованому розголошенню або витоку конфіденційної інформації. Ці рішення зазвичай включають вдосконалені методи сканування даних, алгоритми машинного навчання та налаштовувані параметри політики для виявлення та зменшення потенційних ризиків.

Крім того, DLP-рішення часто надають можливості моніторингу та аудиту, що дозволяє організаціям відстежувати доступ до даних і шаблони використання. Це дозволяє організаціям продемонструвати відповідність і надати докази дотримання нормативних вимог під час аудитів або розслідувань.

Використовуючи надійні хмарні програми безпеки даних, у тому числі DLP, організації можуть ефективно виконувати зобов’язання щодо відповідності та мінімізувати ризик витоку чи порушення даних. Ці заходи сприяють розвитку довіри та впевненості клієнтів, партнерів і регуляторних органів, зрештою покращуючи репутацію організації та допомагаючи уникнути дорогих юридичних і фінансових наслідків.

2.2. Виклики безпеці хмарних середовищ

Хмарні середовища рясніють великою кількістю ризиків, загроз та викликів, яким повинні протидіяти організації, щоб підтримувати безпечну та стійку інфраструктуру. Для їх ефективного подолання вкрай важливо розуміти тонкі відмінності між ризиками, загрозами та викликами безпеці даних та прийняти відповідні стратегії та рішення.

Ризики стосуються потенційних подій або обставин, які можуть мати негативний вплив на безпеку хмари. Це можуть бути витоки даних, несанкціонований доступ, втрата даних, збої в обслуговуванні, порушення відповідності тощо. Оцінка та управління цими ризиками має важливе значення для розробки ефективної стратегії безпеки хмари. Це передбачає виявлення потенційних вразливостей і загроз, оцінку їх потенційного впливу та впровадження заходів пом’якшення, щоб зменшити ймовірність і вплив ризиків [37].

Загрози — це конкретні випадки або умови, які можуть використовувати вразливі місця та завдавати шкоди або порушити роботу хмарного середовища. Загрози можуть виникати з різних джерел, включаючи зловмисників, внутрішні загрози, випадкові інциденти та стихійні лиха. Деякі поширені загрози в хмарних середовищах включають зловмисне програмне забезпечення, атаки соціальної інженерії, DDoS- та APT-атаки і спроби викрадення даних. Захист від цих загроз вимагає впровадження відповідних заходів безпеки, таких як

брандмауери, системи виявлення/запобігання вторгненням, шифрування та рішення моніторингу безпеки.

Виклики хмарній безпеці — це складні проблеми, з якими можуть зіткнутися організації під час експлуатації та захисту свого комплексного середовища. Ці виклики можуть випливати з різних факторів, включаючи динамічну природу хмарних інфраструктур, складність керування контролем доступу між кількома хмарними провайдерами, забезпечення відповідності нормативним вимогам у різних юрисдикціях, а також підтримку видимості та контролю над хмарними ресурсами. Наприклад, керування складними списками контролю доступу (ACL) і забезпечення узгодженої відповідності нормам захисту даних у глобально розподіленій хмарній інфраструктурі є типовими проблемами безпеки хмари. Щоб подолати їх, часто потрібні надійні рішення безпеки, автоматизація та комплексні практики управління безпекою.

Для ефективного управління ризиками, реагування на загрози та подолання викликів у хмарній безпеці організації повинні прийняти цілісний підхід. Це включає впровадження поєднання профілактичних, детективних і реагуючих заходів безпеки, регулярну оцінку стану безпеки, використання аналізу загроз, впровадження строгих політик керування доступом, постійний моніторинг хмарного середовища та сприяння міцній культурі безпеки в усій організації.

Розуміючи та вирішуючи ризики, загрози та виклики у складних середовищах, організації можуть проактивно захищати свої дані, програми та інфраструктуру, забезпечуючи безпечне та стійке хмарне середовище.

Нижче будуть наведені приклади популярних проблем, з якими стикаються організації при використанні хмарних середовищ [38].

Захист стороннього програмного забезпечення та незахищених API

Захист програмного забезпечення сторонніх розробників і незахищених API є важливим завданням для підтримки безпечного середовища. Багато підприємств значною мірою покладаються на софт сторонніх розробників, щоб

покращити свої хмарні середовища та оптимізувати життєві цикли розробки програмного забезпечення. Однак, якщо не керувати належним чином, ці програми і пов’язані з ними API можуть створювати вразливості та розширювати площину атаки.

Однією з ключових проблем є неправильно налаштовані межі дозволів, установлені для програм сторонніх розробників. Дослідження показують, що лише невеликий відсоток підприємств встановлює оптимальні дозволи, тоді як більшість надає надмірні привілеї, які можуть розкрити конфіденційні дані та збільшити ризик неавторизованого доступу.

Ланцюжок постачання програмного забезпечення – ще одна сфера, яка потребує уваги. Програми сторонніх розробників часто взаємодіють і обмінюються даними через API. Якщо ці API небезпечні або неправильно налаштовані, вони можуть стати ціллю зловмисників, щоб використати вразливості та отримати неавторизований доступ. Нещодавня атака на ланцюг поставок SolarWinds [6] є яскравим прикладом ризиків, пов’язаних із вразливим програмним забезпеченням сторонніх розробників. Під час цієї атаки зловмисникам вдалося впровадити шкідливий код у платформу SolarWinds Orion, широко використовуваний інструмент моніторингу та управління інфраструктурою. У результаті численні організації, які використовують платформу, були скомпрометовані, а конфіденційні дані були розкриті протягом тривалого періоду, перш ніж було виявлено атаку.

Щоб вирішити цю проблему, організаціям необхідно впровадити надійні заходи для захисту стороннього програмного забезпечення та API. Це включає проведення ретельної оцінки такого ПЗ перед інтеграцією, забезпечення дотримання найкращих практик безпеки, а також регулярне оновлення та виправлення для пом’якшення вразливостей. Крім того, слід запровадити суворий контроль доступу для API, включаючи механізми автентифікації та авторизації, щоб запобігти несанкціонованому доступу. Постійний моніторинг і аудит стороннього програмного забезпечення та API є важливими для швидкого виявлення будь-яких проблем безпеки.

Вирішуючи ці проблеми та впроваджуючи надійні заходи безпеки, організації можуть мінімізувати ризики, пов’язані зі стороннім програмним забезпеченням і API, підвищити загальну безпеку та підтримувати конфіденційність, цілісність і доступність своїх даних і програм у хмарному середовищі.

Недостатність видимості

Відсутність видимості в хмарних середовищах є серйозною проблемою, з якою можуть зіткнутися організації. Зі швидким розповсюдженням таких ресурсів стає все важче підтримувати повне уявлення про всю хмарну інфраструктуру [39].

Одним із аспектів недостатньої видимості є розростання хмар. Це відбувається, коли організації втрачають контроль над своїми хмарними ресурсами, а активи надаються та розгортаються різними користувачами. Без централізованої видимості стає складно відстежувати ці ресурси та ефективно керувати ними.

Іншим наслідком недостатньої видимості є труднощі з виявленням вразливостей безпеки. З численними одночасними хмарними програмами та технологіями стає складно визначити та вирішити відомі та невідомі проблеми безпеки. Без моніторингу в реальному часі організації можуть не знати про потенційні вразливості, що полегшує їх використання зловмисниками.

Відсутність видимості також впливає на реагування на інциденти. Без належного моніторингу виявлення інцидентів безпеки та реагування на них стає трудомістким процесом із затримкою. Виявлення порушень або підозрілих дій може зайняти більше часу, що призведе до тривалого впливу потенційних загроз. Крім того, відсутність всебічної видимості перешкоджає можливості повного розслідування інцидентів і запровадження відповідних заходів для виправлення ситуації.

Складність IT-середовища та різноманітних програм сторонніх розробників, цифрових ідентифікаторів і конфіденційних даних ще більше

загострюють проблему відсутності видимості. Організаціям необхідно мати цілісне уявлення про обчислювальні платформи, платформи даних, інструменти безпеки та ідентифікації, технології коду, інструменти CI/CD, робочі навантаження та API, щоб ефективно керувати та захищати свої середовища. Без цієї видимості збереження контролю та забезпечення безпеки хмарної інфраструктури стає серйозною проблемою.

Загалом відсутність видимості в хмарних середовищах створює значні ризики для стану безпеки організації. Вирішення цієї проблеми вимагає впровадження заходів для підвищення видимості, таких як розгортання інструментів моніторингу, проведення регулярних оцінок і впровадження централізованих механізмів управління та контролю.

Нестача фахівців з безпеки хмарних середовищ

Дефіцит талантів у сфері кібербезпеки є гострою проблемою, з якою стикаються багато організацій, коли справа доходить до вирішення проблем безпеки в хмарі. Через це компанії часто покладаються на зовнішні ресурси, такі як продукти SaaS і «банки знань», щоб заповнити прогалини в своїх знаннях з безпеки. Однак ця надмірна залежність від зовнішніх рішень може не забезпечити комплексного захисту, необхідного для вирішення складних потреб кібербезпеки в хмарних IT-середовищах.

Відсутність власних фахівців з хмарної безпеки може створити кілька проблем для організацій. Перш за все, без необхідного досвіду компаніям може бути важко повністю зрозуміти унікальні вимоги безпеки та загрози, пов’язані з їх хмарною інфраструктурою. Це може призвести до реактивного підходу до безпеки, коли вразливі місця розглядаються лише після того, як стався інцидент, а не проактивно зменшують ризики [40].

Крім того, відсутність фахівців з хмарної безпеки означає, що організації можуть не мати необхідних навичок і знань для впровадження належних заходів безпеки та керування ними у своїх хмарних середовищах. Це включає такі завдання, як налаштування контролю доступу, захист API, керування

шифруванням і моніторинг підозрілих дій. Без цих основоположних методів безпеки організації більш сприйнятливі до кіберзагроз.

Щоб вирішити ці проблеми, організаціям слід розглянути можливість впровадження ініціатив, які передбачають інтеграцію практик безпеки на ранніх етапах життєвого циклу розробки програмного забезпечення. Надаючи розробникам знання та інструменти для виявлення та усунення вразливостей безпеки з самого початку, організації можуть проактивно пом’якшувати ризики та запобігати впровадженню недоліків безпеки у своїх хмарних програмах.

Глобальна нестача фахівців з кібербезпеки має далекосяжні наслідки. Організації, які погано підготовлені до вирішення викликів хмарної безпеки, можуть зіткнутися з незначними інцидентами, які порушують роботу, компрометують дані або впливають на довіру клієнтів. Однак у серйозних випадках підприємства можуть зіткнутися з катастрофами, що призведуть до значних фінансових втрат, регулятивних штрафів і непоправної шкоди їхній репутації. Витік даних T-Mobile [7], який поставив під загрозу особисту інформацію мільйонів клієнтів, служить яскравим нагадуванням про потенційний масштаб шкоди, з якою можуть зіткнутися організації без належних заходів кібербезпеки.

Враховуючи масштаби дефіциту спеціалістів із кібербезпеки та зростаючу важливість хмарної безпеки, організації повинні вживати проактивних заходів для вирішення цієї проблеми. Це включає інвестиції в програми навчання та розвитку, сприяння співпраці між командами безпеки та розробки, використання інструментів автоматизації та інтеграції для оптимізації процесів безпеки та партнерство із зовнішніми експертами, коли це необхідно. Сформувавши кваліфіковану та обізнану робочу силу, організації можуть ефективно вирішувати унікальні проблеми безпеки, пов’язані з хмарними IT-середовищами, і зменшувати потенційний ризик і вплив інцидентів безпеки.

Управління хмарними даними

Управління хмарними даними є критично важливим аспектом кібербезпеки, оскільки організації все більше покладаються на хмарні платформи для зберігання та обробки величезних обсягів даних. Дані є цінним активом для компаній, і в них міститься конфіденційна інформація, як-от інформація, що дозволяє ідентифікувати особу (PII), захищена інформація про здоров'я (PHI) і дані індустрії платіжних карток (PCI). Щоб забезпечити надійне управління та захист цих активів, організації повинні вирішити кілька проблем [41].

Одним із важливих завдань є досягнення видимості на хмарних платформах, таких як Amazon Web Services (AWS), Google Cloud Platform (GCP) і Microsoft Azure. Організації повинні чітко розуміти свої обсяги даних, місця, де вони зберігаються, і типи баз даних, які вони використовують. Ця видимість є важливою для ефективної безпеки даних і управління.

Ще одна складна проблема – виявлення випадків розкриття даних. Оскільки в хмарі зберігається величезна кількість даних, дуже важливо мати механізми для виявлення будь-якого несанкціонованого доступу або витоку даних. Це вимагає постійного моніторингу та аналізу журналів доступу, мережевого трафіку та інших показників доступу до даних.

Розуміння потоку даних і походження також є важливим аспектом управління хмарними даними. Організаціям необхідно відстежувати рух даних у своїх хмарних середовищах, зокрема те, як вони збираються, зберігаються, обробляються та передаються. Це допомагає встановити підзвітність даних і підтримує відповідність нормативним вимогам, таким як Загальний регламент захисту даних (GDPR) і Закон про перенесення та підзвітність медичного страхування (HIPAA).

Впровадження та забезпечення дотримання політик управління даними є ще одним викликом у хмарних середовищах. Організації повинні визначити чіткі вказівки та процедури обробки даних, контролю доступу, шифрування та

збереження. Ці політики необхідно послідовно застосовувати на всіх хмарних платформах і службах, щоб забезпечити єдину та надійну структуру керування даними.

Дотримання вимог також є важливим аспектом управління хмарними даними. Організації повинні переконатися, що їх методи обробки даних відповідають відповідним нормам і галузевим стандартам. Це включає регулярні оцінки, аудити та звітність, щоб продемонструвати відповідність таким структурам, як HIPAA, GDPR і стандарт безпеки даних індустрії платіжних карток PCI DSS.

Нарешті, життєво важливо визначити та усунути шляхи атак, які можуть призвести до розкриття конфіденційних даних. Хмарні середовища можуть бути складними, з різними взаємопов'язаними службами та конфігураціями. Компанії повинні проводити ретельну оцінку ризиків, тести на проникнення та сканування вразливостей, щоб виявити потенційні слабкі місця в налаштуваннях хмари та завчасно їх усунути.

Наслідки збоїв в управлінні даними можуть бути значними та тривалими. Gartner прогнозує [8], що до 2025 року 80% підприємств не зможуть розвивати свої цифрові операції через неоптимальне управління даними. Це підкреслює важливість надання пріоритету надійним практикам керування хмарними даними для захисту конфіденційної інформації, дотримання нормативних вимог і підтримки зростання бізнесу та інновацій.

Щоб вирішити ці проблеми, організації повинні інвестувати в комплексні стратегії керування хмарними даними. Це включає використання вбудованих у хмару інструментів і служб безпеки, впровадження механізмів класифікації даних і контролю доступу, застосування методів шифрування та токенізації, а також використання рішень для запобігання втраті даних. Крім того, регулярний перегляд і оновлення політики управління даними, забезпечення безперервного навчання та програм підвищення обізнаності для співробітників, а також підтримка культури пильності безпеки можуть допомогти зменшити ризики та покращити управління хмарними даними.

Тіньове IT

Тіньове IT – це використання IT-ресурсів або програмних додатків, які не схвалені або не керуються IT-відділом або групою безпеки організації. Це поширене явище, яке виникає в гнучких робочих середовищах, де розробники та команди можуть обходити традиційні процеси, щоб швидко та незалежно отримувати доступ до IT-ресурсів і використовувати їх [42].

Ці незатверджені ресурси можуть включати послуги «Інфраструктура як послуга» (IaaS), «Платформа як послуга» (PaaS) і «Програмне забезпечення як послуга» (SaaS), API (інтерфейси прикладного програмування), сервери та апаратне забезпечення. Це явище може варіюватися від окремих співробітників, які використовують несанкціоноване програмне забезпечення, до цілих команд або відділів, які покладаються на несхвалені хмарні служби для своєї роботи.

Хоча тіньове IT може забезпечити переваги з точки зору гнучкості та продуктивності, вони також становлять значні ризики, особливо з точки зору безпеки даних. Коли дані зберігаються або обробляються поза схваленою IT-інфраструктурою чи заходами безпеки, вони стають більш уразливими до несанкціонованого доступу, витоку даних або порушень відповідності.

Організації повинні вжити заходів для вирішення проблеми тіньових IT та пом’якшити потенційні ризики, пов’язані з ними. Це може передбачати покращення зв’язку та співпраці між IT-командами та бізнес-підрозділами для виявлення та усунення основних причин тіньових IT, надання альтернативних схвалених рішень, які відповідають потребам співробітників, проведення регулярних оцінок безпеки та аудитів, а також встановлення політики та вказівок щодо використання ресурсів IT.

Визнаючи поширеність тіньового IT і вживаючи профілактичних заходів, організації можуть знайти баланс між гнучкістю та інноваціями, зберігаючи при цьому контроль, безпеку та відповідність своїй IT-інфраструктурі та даним.

Управління поверхнею атак, що швидко розвивається

Управління поверхнею атак, що швидко розвивається, є серйозною проблемою для організацій, які використовують хмарні обчислення. Масштабованість і економічна ефективність, які пропонуються хмарними службами, дозволяють підприємствам швидко розширювати свою інфраструктуру та можливості. Однак це зростання також призводить до збільшення поверхні атаки, створюючи більше можливостей для потенційних порушень безпеки.

Поверхня атаки відноситься до різних точок вразливості, які існують в IT-інфраструктурі організації. У контексті хмарних обчислень поверхня атаки розширюється, оскільки додається більше хмарних ресурсів, включаючи ідентифікатори людей і служб, віртуальні машини, безсерверні функції, пристрої, робочі навантаження, що не підлягають агентуванню, служби інфраструктури як коду (IaC) і дані.

Ці хмарні ресурси чутливі до широкого спектру ризиків безпеки. Надмірні права доступу, наприклад, виникають, коли користувачі або служби мають надмірні дозволи на доступ, що потенційно може призвести до несанкціонованого доступу або підвищення привілеїв. Випадкове оприлюднення секретів і ключів доступу може відкрити конфіденційну інформацію та дозволити зловмисникам отримати несанкціонований доступ. Слабкі паролі створюють можливості для атак грубої сили або крадіжки облікових даних. Неправильні конфігурації, такі як неправильне налаштування елементів керування доступом або залишення відкритих портів, створюють вразливі місця в безпеці.

Управління ризиками, пов’язаними з розширеною та динамічною поверхнею атак, життєво важливо для організацій. Однак вони не можуть дозволити собі уповільнити свою роботу або пожертвувати гнучкістю заради вирішення цих проблем. Традиційних підходів до безпеки, таких як ручний аудит або статичні заходи безпеки, недостатньо в цьому ландшафті, що швидко розвивається [43].

Щоб ефективно керувати поверхнею атак, організації повинні прийняти динамічні та проактивні методи безпеки. Це включає впровадження безперервного моніторингу безпеки та механізмів виявлення загроз, які можуть ідентифікувати потенційні порушення безпеки та реагувати на них у режимі реального часу. Автоматизовані інструменти оцінки безпеки можуть допомогти виявити неправильні конфігурації та вразливості, дозволяючи швидко виправити їх.

Крім того, організації повинні надати пріоритет встановленню та застосуванню суворої політики контролю доступу. Використання таких механізмів, як найменші привілеї, контроль доступу на основі ролей і багатофакторна автентифікація, може зменшити ризики, пов’язані з надлишковими правами доступу та слабкими обліковими даними.

Регулярні перевірки безпеки, оцінки та навчання співробітників також мають вирішальне значення для підтримки належним чином захищеної поверхні для атак. Постійне навчання передовим практикам і новим загрозам допомагає співробітникам зрозуміти свою роль у підтримці безпечного хмарного середовища.

Зрештою, управління ризиками, пов’язаними з розширенням поверхні атаки, вимагає проактивної та постійної стратегії безпеки. Поєднуючи автоматизацію, безперервний моніторинг, заходи контролю доступу та навчання співробітників, організації можуть підтримувати оперативну гнучкість, зводячи до мінімуму потенційні порушення безпеки у своїй хмарній інфраструктурі.

Безпека комплексних хмарних середовищ

Безпека комплексних хмарних середовищ є складним аспектом хмарних обчислень. У міру того, як організації все більше застосовують мультихмарні стратегії, ландшафт безпеки стає складнішим, що загострює проблеми, властиві хмарним інфраструктурам.

У мультихмарному середовищі компанії використовують кілька постачальників хмарних послуг, створюючи різноманітну та розподілену

інфраструктуру. Хоча цей підхід пропонує такі переваги, як уникнення прив'язки до постачальника та використання спеціалізованих послуг від різних постачальників, він також створює додаткові складності та ризики.

Однією з головних проблем безпеки в багатохмарному середовищі є керування ідентифікацією та доступом (IAM) і контроль доступу. Вирішальним стає чітке розуміння того, хто має доступ до яких хмарних ресурсів і чому. Без належного керування IAM організації не можуть виявити потенційні вразливості, передбачити шляхи атак і оцінити потенційний вплив інциденту безпеки на свою мультихмарну інфраструктуру [44].

Забезпечення узгоджених політик і елементів керування IAM у різних хмарних провайдерів може бути складним завданням. Кожен хмарний постачальник може мати власні унікальні можливості IAM, API та конфігурації, що вимагає від організацій керування та синхронізації кількох сховищ ідентифікаційної інформації. Ця складність збільшує ймовірність неправильної конфігурації або прогалин у контролі доступу, що може призвести до несанкціонованого доступу або витоку даних.

Крім того, підтримання видимості та безпеки в кількох середовищах є складним завданням. Організаціям необхідні комплексні інструменти моніторингу та безпеки, які можуть у реальному часі надавати інформацію про стан безпеки та дії в кожному хмарному середовищі. Прогалини у видимості можуть виникати, коли різні постачальники мають різні рівні прозорості та можливостей моніторингу, що ускладнює послідовне виявлення загроз і реагування на них.

Відповідність і управління даними також стають складнішими в багатохмарному середовищі. Різні постачальники хмарних послуг можуть мати різні вимоги до відповідності та сертифікати, тому зрозуміти, як дані зберігаються, як організовано доступ до них і як захищаються в кількох хмарах може бути складно. Організації повинні переконатися, що вони мають відповідні засоби контролю та процеси для підтримки відповідності та захисту

конфіденційних даних під час їх переміщення між різними хмарними платформами.

Загалом ефективна багатохмарна безпека потребує проактивного та цілісного підходу, який розглядає питання керування IAM, видимості, відповідності та керування даними в усіх хмарних середовищах. Впроваджуючи надійні заходи безпеки та використовуючи відповідні інструменти та технології, організації можуть мінімізувати ризики та проблеми, пов’язані з комплексною інфраструктурою, одночасно максимізуючи її переваги.

2.2.1. Безпека хмарного середовища - спільна відповідальність

У контексті хмарної безпеки як постачальник хмарних послуг, так і клієнт несуть спільну відповідальність. Хоча CSP відповідає за безпеку хмарного середовища та забезпечення відповідності платформи та послуг, які вони надають, клієнти повинні розуміти свою роль у захисті власних даних і програм [45].

Клієнти часто роблять помилку, припускаючи, що CSP несе повну відповідальність за безпеку, що може призвести до більш зневажливого ставлення при впровадженні заходів безпеки. Однак уразливості в хмарній безпеці часто є результатом неправильних практик і неправильних налаштувань з боку клієнта.

Рівень відповідальності за хмарну безпеку залежить від типу хмарного сервісу, який використовується. Незалежно від того, чи це розгортання загальнодоступної, приватної чи гібридної хмари, клієнти повинні взяти на себе відповідальність за захист своїх операційних систем, програм і мережевого трафіку. Їм потрібно запровадити жорсткі політики, засоби контролю доступу та безпечні конфігурації для захисту своїх даних.

Для клієнтів важливо розуміти, які дані зберігаються в хмарі, хто має до них доступ і які внутрішні засоби захисту використовуються. Вони повинні

знати про зобов’язання CSP щодо безпеки та межі своєї відповідальності. Ці знання дають організаціям змогу приймати обґрунтовані рішення та за потреби впроваджувати додаткові заходи безпеки.

Подібним чином, забезпечення відповідності даних є спільною відповідальністю. У той час як постачальники послуг прагнуть забезпечити відповідність своїх платформ і послуг галузевим стандартам і нормам, клієнти повинні забезпечити відповідність своїх власних програм, даних і будь-яких сторонніх служб, якими вони користуються. Це може включати постійний моніторинг, регулярне тестування та періодичний аудит хмарних операцій для підтримки нормативної відповідності.

Щоб відповідати нормам безпеки, компанії повинні розуміти, як галузеві стандарти та державні норми впливають на їхні хмарні процеси та дані. Вони повинні ознайомитися з конкретними вимогами та забезпечити відповідність своїх хмарних операцій цим стандартам.

Таким чином, як CSP, так і клієнт поділяють відповідальність за безпеку та відповідність хмарі. Розуміючи свої ролі та працюючи разом, вони можуть створити безпечне та сумісне хмарне середовище для зберігання та обробки конфіденційних даних.

2.3. Відповідність вимогам стандартів

Коли компанія перебуває в хмарі, їй слід потурбуватися про те, як постачальник послуг може допомогти дотримуватися законів, таких як Європейський загальний регламент захисту даних (GDPR) [46] або HIPAA [47] у США. Це обговорення має відбутися на самому початку міграції у хмарне середовище.

Компанії іноді опиняються в хмарі задовго до того, як планували це зробити, і це ускладнює ситуацію. Одним із основних принципів таких

середовищ є те, що має існувати інтерфейс самообслуговування, щоб клієнту було легко налаштувати та за необхідності змінити конфігурацію ресурсів.

Однак не ясно, хто в компанії замовника буде це робити. Як виявилося, сьогодні це може бути будь-хто. Все, що потрібно, це корпоративна кредитна картка, і відділ може почати перегони, розміщуючи дані в хмарі. Термін для цього не новий - це тіньове IT. Сьогодні цей термін широко використовується через особливості хмарних середовищ.

Відповідність стандартам – це дотримання нормативних і галузевих правил і вимог постачальників і клієнтів для забезпечення безпеки, конфіденційності та відповідності законодавству даних, пов’язаних програм, а також того, як дані зберігаються й обробляються в хмарному середовищі.

Загалом, ця відповідність стосується дотримання певних правил, стандартів і найкращих практик, розроблених для забезпечення безпеки та конфіденційності даних, що зберігаються та обробляються в хмарних середовищах. Крім того, цей процес передбачає впровадження необхідних адміністративних і технічних засобів контролю для захисту інформації, систем і програм від несанкціонованого доступу, порушень даних та інших ризиків безпеки.

Дотримання галузевих норм, таких як Закон про перенесення та підзвітність медичного страхування (HIPAA) для галузі охорони здоров’я, Стандарт безпеки даних платіжних карток (PCI DSS) для організацій, що обробляють інформацію про кредитні картки, або Загальні правила захисту даних (GDPR) щодо захисту даних громадян Європейського Союзу – це лише деякі з багатьох правил, яких організаціям, можливо, доведеться дотримуватися.

Відповідність стандартам стосується практик і заходів, запроваджених для забезпечення відповідності використання хмарних служб галузевим нормам, стандартам безпеки та найкращим практикам. Оскільки організації все більше покладаються на хмарну інфраструктуру та сервіси, вкрай важливо

вирішувати проблеми безпеки та відповідності, які виникають у цьому середовищі.

Коли організації переносять свої системи, інфраструктуру та програми в хмару, вони, по суті, довіряють свої дані постачальнику хмарних послуг (CSP). Це створює нові ризики, оскільки дані зберігаються в спільній інфраструктурі та доступ до них здійснюється віддалено. Щоб пом'якшити ці ризики, CSP пропонують різні функції безпеки та елементи керування.

Наприклад, CSP реалізують шифрування даних як під час передачі, так і в стані спокою, щоб захистити дані від несанкціонованого доступу. Вони також забезпечують надійні можливості ідентифікації та керування доступом, гарантуючи, що лише авторизовані користувачі можуть отримати доступ до даних і ресурсів у хмарі. Контроль доступу до мережі, наприклад брандмауери та віртуальні приватні мережі (VPN), використовуються для захисту хмарного середовища від зовнішніх загроз.

На додаток до цих заходів безпеки, CSP проводять регулярний моніторинг безпеки, щоб виявити та реагувати на будь-які потенційні порушення безпеки або вразливості. Цей постійний процес допомагає гарантувати, що хмарне середовище залишається безпечним і сумісним.

Постачальники послуг також відповідають за дотримання галузевих норм і стандартів. Вони проходять незалежні перевірки та сертифікації, які перевіряють їх дотримання вимог, викладених у таких нормативних актах, як Загальний регламент захисту даних (GDPR), Закон про перенесення та підзвітність медичного страхування (HIPAA) або Стандарт безпеки даних індустрії платіжних карток (PCI DSS), серед інших. Ці сертифікати гарантують своїм клієнтам, що CSP запровадив необхідні засоби контролю та захисту для захисту даних і підтримки відповідності.

Використовуючи ресурси та можливості CSP, організації можуть ефективніше досягти бажаного стану безпеки. Вони можуть покладатися на досвід та інвестиції, зроблені CSP у впровадженні надійних засобів контролю

безпеки та відповідності вимогам. Це дозволяє організаціям зосередитися на своєму основному бізнесі, одночасно використовуючи переваги хмари, знаючи, що їхні дані безпечні та відповідають вимогам.

Загалом відповідність хмарним вимогам має важливе значення для того, щоб організації могли впевнено використовувати хмарні сервіси, дотримуючись нормативних вимог і вимог безпеки. Працюючи з CSP, які надають пріоритет відповідності та безпеці, організації можуть отримати переваги від масштабованості, гнучкості та економічності хмари без шкоди для захисту даних і дотримання нормативних вимог.

2.3.1. Стандарти безпеки хмарних середовищ

Оскільки організації продовжують переносити свої навантаження в хмару, вони стикаються з декількома проблемами, головною з яких є безпека. Компанії повинні переконатися, що їхні конфіденційні дані в безпеці та відповідають різним стандартам і нормам.

Хмара є привабливою мішенню для кібератак через її доступ до загальнодоступних мереж і задокументованих знань, які мають зловмисники щодо використання хмарних середовищ. Складність хмарних конфігурацій, включаючи віртуальні машини, безсерверні функції, контейнери та сховища ще значно збільшує поверхню загроз [48].

Як постачальникам хмарних послуг, так і користувачам хмарних технологій важко визначити необхідні заходи для забезпечення безпечного середовища. Хоча існують дослідницькі організації, найкращі методи безпеки та нормативні вимоги, загальновизнаного стандарту справді безпечного хмарного середовища не існує.

Це підкреслює важливість для компаній прийняти всеосяжну структуру, яка стосується всіх аспектів хмарної безпеки. Вона повинна охоплювати такі сфери, як керування ідентифікацією та доступом (IAM), безпека мережі,

безпека віртуалізації, доступ до мережі з нульовою довірою (ZTNA), безпека кінцевих пристроїв, конфіденційність даних і безпека вмісту.

Впроваджуючи та дотримуючись надійної хмарної системи безпеки, підприємства можуть зменшити ризики, пов’язані з хмарними обчисленнями. Це дасть їм впевненість у тому, що їхні дані захищено, а їхні операції можуть продовжуватися без шкоди для вимог безпеки чи відповідності.

Далі буде розглянуто популярні стандарти та регуляції, вимог яких необхідно дотримуватись задля забезпечення високого рівня надійності збереження інформації.

NIST 800-53

Контроль безпеки Національного інституту стандартів і технологій (NIST) 800-53 зазвичай застосовується до Федеральних інформаційних систем США. Останні, як правило, повинні пройти офіційний процес оцінки та авторизації, щоб забезпечити достатній захист конфіденційності, цілісності та доступності інформації та інформаційних систем [49].

NIST Cybersecurity Framework (CSF) підтримується урядами та галузями в усьому світі як рекомендований базовий рівень для використання будь-якою організацією, незалежно від її сектора чи розміру. За даними Gartner, у 2015 році CSF використовували приблизно 30 відсотків організацій США, а до 2020 року, за прогнозами, використання досягне 50 відсотків. Починаючи з 2016 фінансового року, показники Федерального агентства щодо модернізації інформаційної безпеки (FISMA) були організовані навколо CSF, і тепер агентства зобов’язані впроваджувати CSF згідно з Указом про кібербезпеку [9].

Кожен контроль у межах CSF зіставляється з відповідними елементами контролю NIST 800-53 у рамках Федеральної програми управління ризиками та авторизацією США (FedRAMP).

FedRAMP було створено, щоб забезпечити стандартизований підхід до оцінки, моніторингу та авторизації продуктів і послуг хмарних обчислень. FedRAMP базується на стандарті NIST SP 800-53, доповненому елементами

управління FedRAMP і вдосконаленнями керування. Такі постачальники послуг хмарних обчислень, як Azure і AWS мають тимчасовий дозвіл FedRAMP високого рівня на роботу, виданий Спільною авторизаційною радою (JAB) FedRAMP. Враховуючи тісне узгодження між засобами контролю NIST CSF і NIST SP 800-53, існуючі повноваження FedRAMP High забезпечують повну впевненість клієнта в тому, що послуги в області аудиту FedRAMP відповідають практикам управління ризиками NIST CSF [10].

ISO 27017

ISO/IEC 27017 — це стандарт інформаційної безпеки для організацій, які використовують (або планують використовувати) хмарні сервіси. Постачальники хмарних послуг повинні відповідати цьому стандарту, оскільки він забезпечує безпеку їхніх клієнтів та послуг, забезпечуючи послідовний і комплексний підхід до інформаційної безпеки. Цей міжнародний стандарт пропонує настанови для споживачів хмарних послуг і постачальників, які сприяють реалізації засобів керування. Структура визначає узгодження управління безпекою для хмарних обчислень, віртуальних і фізичних мереж.

ISO 27017 вживає всіх необхідних заходів безпеки, аналізу на основі ризиків для онлайн-безпеки та поширює їх безпосередньо на хмарну безпеку, де застосовуються засоби контролю інформаційної безпеки.

Для клієнтів важливо мати впевненість у безпеці своїх даних у хмарі. ISO/IEC 27017 — це всесвітньо визнаний стандарт, який ефективно зменшить імовірність витоку даних і підвищить довіру користувачів, демонструючи прихильність постачальника послуг до технологій інформаційної безпеки. Описані в документі пункти допоможуть вирішити різні питання, включаючи право власності на активи, видалення та повернення активів після розірвання клієнтського контракту та безпеку віртуального середовища клієнта [11].

ISO 27018

ISO 27018 охоплює захист персональної інформації (PII) у загальнодоступних хмарах, які служать процесорами PII. Незважаючи на те, що

цей стандарт особливо спрямований на постачальників публічних хмарних послуг, таких як AWS або Azure, контролери ідентифікаційної інформації (такі як постачальник SaaS, який обробляє ідентифікаційну інформацію клієнта в AWS) несуть певну відповідальність. Відповідність цьому документу демонструє клієнтам, що постачальник послуг має систему контролю, яка спеціально спрямована на захист конфіденційності їх даних [12].

CIS Controls

Організації можуть захистити свої системи за допомогою засобів керування Internet Security Center (CIS), які є політиками з відкритим вихідним кодом, заснованими на консенсусі. Кожна перевірка ретельно контролюється кількома експертами, перш ніж зробити висновок.

Щоб легко отримати доступ до списку оцінок для хмарної безпеки, необхідно звернутися до CIS Benchmarks, налаштованих для конкретних постачальників хмарних послуг. Наприклад, можна використовувати елементи керування CIS-AWS, набір елементів керування, створений спеціально для робочих навантажень за допомогою Amazon Web Services (AWS).

CIS Controls framework може допомогти підготуватися до аудитів. Він містить попередньо зібрану колекцію елементів керування з описами та процедурами тестування. Ці елементи керування згруповані в набори відповідно до вимог CIS.

Використовуючи структуру як відправну точку, можна створити оцінку керівника аудиту та почати збирати докази, які мають відношення до аудиту. Після створення оцінки Audit Manager починає оцінювати ресурси AWS. Це робиться на основі елементів керування, визначених у рамках CIS Controls v7.1 IG1. Коли настане час для перевірки, буде змога переглянути зібрані докази, а потім додати їх до звіту про оцінку. Також можна використовувати цей звіт про оцінку, щоб показати, що елементи керування працюють належним чином [13].

HIPAA

Закон про перенесення та підзвітність медичного страхування (HIPAA), прийнятий Конгресом США для захисту індивідуальної медичної інформації, також містить частини, які стосуються інформаційної безпеки. Компанії, які обробляють медичні дані, повинні дотримуватися закону HIPAA. Правило безпеки HIPAA (HSR) є найкращим вибором з точки зору безпеки інформації. HIPAA HSR визначає правила захисту електронної особистої інформації про здоров'я людей, яку охоплена організація створює, отримує, використовує або зберігає.

Організаціям, які підпадають під дію правил HIPAA, потрібна оцінка ризиків і плани управління ризиками, щоб зменшити загрози доступності, конфіденційності та цілісності важливих даних про здоров'я, якими вони керують. Припустимо, що компанія надсилає та отримує дані про здоров'я через хмарні служби (SaaS, IaaS, PaaS). Якщо так, то керівництво несе відповідальність за те, щоб постачальник послуг дотримувався норм HIPAA і компанія застосувала найкращі методи керування налаштуваннями хмари.

Технічно не існує такого поняття, як хмарна інфраструктура, сумісна з HIPAA, оскільки жоден хмарний сервер не може бути дійсно сумісним з HIPAA. Відповідність HIPAA залежить від дій людей. Навіть якщо для захисту ePHI у хмарі застосовано належну безпеку, якщо організації охорони здоров'я неправильно налаштують параметри або не запровадять належний контроль доступу, ePHI може бути легко розкрито через Інтернет, порушуючи правила HIPAA.

Тим не менш, багато CSP пропонують хмарне сховище, сумісне з HIPAA, організаціям, які регулюються HIPAA. Це означає, що послуга, яку вони пропонують, включає всі необхідні засоби контролю безпеки для забезпечення конфіденційності, цілісності та доступності ePHI та запобігання недозволеному розголошенню. Ці елементи керування застосовуються до ePHI у стані спокою (зберігаються на хмарних серверах) і в русі до та з хмарного сервера чи служби. Контроль доступу можна налаштувати так, щоб обмежити доступ до ePHI, щоб

лише авторизовані особи могли переглядати, змінювати або передавати дані, а журнали аудиту ведуться для успішних і невдалих спроб доступу та будь-яких змін до ePHI.

Постачальник хмарних послуг, сумісний із HIPAA, гарантує, що в платформу включено засоби захисту, щоб забезпечити її використання відповідно до HIPAA; однак кожна організація, яка регулюється HIPAA, має переконатися, що засоби керування правильно налаштовані та послуга використовується у спосіб, який відповідає правилам конфіденційності та безпеки HIPAA [14].

SOC 2

Форма аудиту операційних процесів, які використовують IT-підприємства, які пропонують будь-які послуги, відома як «Аудит послуг і організації 2» (SOC 2). Світовим стандартом для систем управління ризиками кібербезпеки є звітність SOC 2. Політика, методи та засоби контролю вашої компанії відповідають п’яти принципам довіри, як показано в звіті про аудит SOC 2. У звіті про аудит SOC 2 перераховано безпеку, доступність, цілісність обробки, конфіденційність і конфіденційність як принципи безпеки [50].

SOC 2 – це не стандартна вимога для хмарних провайдерів. Однак перевірений звіт про відповідність є цінним досягненням, оскільки він демонструє прагнення до захисту даних. Це свідчить про те, що постачальник хмарних послуг ефективно впроваджує найкращі галузеві практики.

Клієнти можуть вимагати від постачальника хмарних послуг підтримувати відповідність SOC 2. Проте, навіть якщо це не обов’язкова вимога, аудиторський звіт є перевіреним доказом заходів щодо захисту даних. Це також може бути вирішальним фактором, коли потенційні клієнти обирають постачальника хмарних послуг для ведення бізнесу.

SOC 2 може стати основою для подальших стандартів відповідності. Хмарні постачальники, які відповідають стандарту SOC 2, можуть легше прийняти інші стандарти захисту даних і безпеки. Наприклад, звіт може містити

додатковий розділ для засобів контролю, пов’язаних із Правилами безпеки HIPAA. Вибір постачальника хмарних послуг, який відповідає відповідним нормам, таким як HIPAA, PCI та GDPR, має вирішальне значення для досягнення потенційними клієнтами власних цілей відповідності.

Для хмарних провайдерів оцінка SOC 2 майже напевно включатиме операційні, технічні вимоги та вимоги безпеки, пов’язані з критеріями «безпеки» та «доступності». Інші TSC можуть бути включені до сфери застосування на основі послуг, які вони надають, і цілей постачальника. Оцінка «цілісності обробки», «конфіденційності» та «доступності» є необов’язковою, але вона надає цінну інформацію для персоналу безпеки.

Оскільки все більше компаній переходять на хмарні обчислення, потреба в безпеці даних і атестації відповідності також змінюється. Однак ми можемо бути впевнені, що дотримання нормативних вимог все більше ставатиме стандартом для компаній, які працюють у хмарі. Ми можемо бути впевнені в цьому, тому що великі імена в хмарних службах, включаючи AWS і Azure, лідирують у безпеці даних і відповідності.

Висновки до другого розділу

Хоча переваги хмарних обчислень незаперечні, важливо усунути потенційні ризики, які супроводжують цю технологію. У розділі було розглянуто питання важливості побудови безпечного хмарного середовища та випробування, з якими стикаються адміністратори при розробці заходів безпеки. Неправильна конфігурація, наприклад, може призвести до вразливостей та несанкціонованого доступу до конфіденційних даних. Крім того, ландшафт загроз, що постійно розвивається, створює постійний ризик кібератак на хмарні середовища. Щоб пом’якшити ці ризики, надзвичайно важливо визначити пріоритет безпеки хмари.

Заходи безпеки в хмарі спрямовані на посилення захисту цифрових активів і забезпечення конфіденційності, цілісності та доступності даних у хмарі. Впроваджуючи надійні практики та технології безпеки, організації можуть мінімізувати ймовірність людських помилок або ненавмисних порушень. Це включає використання надійних засобів контролю доступу, шифрування, регулярні оцінки безпеки та ретельний моніторинг для виявлення потенційних загроз і оперативного реагування на них.

Наявність ефективних заходів безпеки в хмарі забезпечує компаніям спокій, запевняючи їх, що їхні дані та операції захищені. Зменшуючи ризик шкідливого порушення, організації можуть зберегти свою репутацію, захистити довіру клієнтів і уникнути фінансових втрат, пов’язаних із компрометацією даних.

Підсумовуючи, хмарні обчислення пропонують компаніям безпрецедентні можливості для зростання, гнучкості та зручності. Однак ці переваги повинні супроводжуватися надійною хмарною безпекою для захисту від потенційних загроз і вразливостей. Приділяючи пріоритет хмарній безпеці, організації можуть забезпечити постійну ефективність своїх хмарних середовищ і використовувати весь потенціал цієї трансформаційної технології.

РОЗДІЛ 3
ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ КОНТРОЛЮ ВІДПОВІДНОСТІ КОНФІГУРАЦІЙ БЕЗПЕКИ СТАНДАРТАМ

3.1. Актуальні загрози безпеці хмарних середовищ

В епоху цифрової трансформації хмарні обчислення стали незамінною технологією як для окремих людей, так і для компаній. Використання таких хмарних служб революціонізувало спосіб зберігання інформації, доступу до неї та спільного використання, забезпечивши безпрецедентну зручність і масштабованість. Проте, оскільки організації все частіше довіряють свої конфіденційні дані хмарі, виникає серйозне занепокоєння – постійно розвивається ландшафт загроз безпеки хмари.

Оскільки кіберзлочинці використовують все більш витончену тактику для використання вразливостей, захист даних у хмарному середовищі став обов’язковим для компаній будь-якого розміру. Цей розділ заглиблюється у сферу хмарної безпеки, розкриваючи існуючі загрози, якими повинні протистояти організації, намагаючись захистити свою конфіденційну інформацію.

Завдяки дослідженню [51] поширених викликів хмарній безпеці, зокрема витоку даних, несанкціонованого доступу, інсайдерських загроз і вразливості спільних ресурсів, цей роздлі має на меті пролити світло на серйозність ризиків, з якими стикаються компанії, що працюють на цифровому кордоні. Крім того, це підкреслить важливість впровадження надійних заходів безпеки та найкращих практик для зміцнення хмарної інфраструктури та запобігання можливим порушенням.

Хоча хмара пропонує величезні переваги з точки зору масштабованості, гнучкості та економічності, вона також являє унікальний набір проблем безпеки. Компанії повинні усвідомлювати важливість випередження цих загроз

та продовжувати працювати над підвищенням безпеки хмарних платформ. Покращуючи розуміння ризиків і створюючи середовище пильності, користувачі можуть і надалі захищати конфіденційну інформацію їх компаній, а також довіру та конфіденційність глобально розподіленої бази клієнтів.

Ландшафт загроз безпеці хмарних середовищ постійно представляє нові небезпеки, що вимагає постійної пильності та адаптації.

Головною серед цих проблем була втрата та витік даних. Згідно зі звітом Statista [15], приголомшливі 64 відсотки респондентів відзначили втрату та витік даних як основну проблему безпеки хмари у 2021 році. Втрата даних може статися через різні причини, включаючи випадкове видалення, зловмисні атаки та навіть стихійні лиха. Витік даних, з іншого боку, зазвичай відбувається, коли дані стають доступними для неавторизованих осіб випадково або спеціально. Викрадення даних хмарного сховища відбувається, коли конфіденційна інформація оприлюднюється, переглядається або використовується особою за межами операційного середовища організації. У звіті зазначено, що часто викрадення даних може відбуватися без відома власника. У деяких випадках власник може не знати про крадіжку даних, поки його не сповістить злодій або поки вони не з’являться у продажу в Інтернеті.

Хоча хмара може бути зручним місцем для зберігання даних, вона також пропонує кілька способів їх викрадення. Щоб захиститися від викрадення, організації почали звертатися до моделі нульової довіри, де використовуються елементи керування безпекою на основі ідентичності для забезпечення найменш привілейованого доступу до даних.

Іншою важливою проблемою було випадкове розкриття облікових даних. Оскільки все більше компаній переносять свою діяльність у хмару, зростає ризик випадкового розкриття хмарних служб зберігання даних і баз даних, що призводить до несанкціонованого доступу. Це може бути особливо шкідливим, якщо дані містять конфіденційну інформацію або призводять до подальших вторгнень у систему.

Неправильно налаштовані параметри безпеки часто спричиняють порушення цілісності даних [52]. Крім того, багато корпоративних методологій керування хмарною безпекою не забезпечують належного захисту хмарної інфраструктури. На це впливають різні речі. Оскільки хмарна інфраструктура призначена для того, щоб бути зручною для користувачів і полегшувати простий обмін даними для компаній, забезпечення того, що дані доступні лише авторизованим сторонам, може бути проблемою. Таким чином, підприємства, які використовують хмарну інфраструктуру, повинні покладатися на заходи безпеки, надані їх постачальником хмарних послуг, щоб встановити та захистити свої хмарні установки. Організаціям, які використовують хмарну інфраструктуру, також потрібна повна видимість і контроль над своєю інфраструктурою. У разі порушення безпеки або неправильної конфігурації хмарні ресурси організації легко залишаються вразливими для зловмисників, оскільки багато організацій не мають досвіду захисту хмарної інфраструктури та часто розгортають кілька середовищ, кожне з яких має унікальний набір засобів безпеки, наданих постачальником.

Ін’єкції зловмисного програмного забезпечення є одними з популярних вразливостей хмарних інфраструктур. Це сценарії або фрагменти коду, які додаються до хмарних служб і проявляють себе як «законні екземпляри» під час роботи як SaaS із хмарних серверів. Це означає, що шкідливий код може бути введений у хмарні служби та сприйматися як компонент програми чи служби, що працює на самих хмарних серверах.

Зловмисники можуть підслуховувати, ставити під загрозу цілісність особистих даних і викрадати їх після завершення впровадження шкідливого програмного забезпечення. І хмара почала працювати разом з ним. У звіті Університету Східної Кароліни [16] про загрози безпеці в хмарних обчисленнях ризики безпеки аналізуються ризики встановлення зловмисного програмного забезпечення для проблем безпеки хмарних обчислень. Як висновок, «впровадження зловмисного програмного забезпечення стало ключовою проблемою безпеки в системах хмарних обчислень».

Відсутність видимості мережевих операцій є недоліком переходу від локальної архітектури зберігання даних до хмарної інфраструктури. Таким чином перед нами постає чергова проблема. Підприємства надають CSP різний ступінь контролю над своєю IT-інфраструктурою в обмін на такі переваги, як економія коштів і легка масштабованість із наданням сховища на вимогу. Вид моделі надання послуг визначає, який контроль мають постачальники і які зобов'язання щодо безпеки даних мають підприємства. Однак відсутність розуміння хмарних середовищ створює постійну загрозу для компаній, які залежать від них для управління критично важливими даними, незалежно від моделі спільної відповідальності.

Інтерфейси прикладного програмування (API) дозволяють клієнтам персоналізувати роботу з інструментами безпеки в хмарі. Однак сама природа API може становити загрозу для безпеки хмари. Вони автентифікують, надають доступ і впроваджують шифрування, дозволяючи компаніям налаштовувати функції своїх хмарних інфраструктурних служб відповідно до потреб свого бізнесу. Загрози безпеці зростають, коли інфраструктура API розширюється, щоб пропонувати кращі послуги. API дають розробникам інструменти для створення своїх програм та інтеграції їх з іншим критично важливим програмним забезпеченням. Наприклад, розробники можуть використовувати YouTube як добре відомий і простий приклад API для включення YouTube у свої веб-сайти чи програми. Уразливість API полягає в спілкуванні, яке відбувається між програмами. Незважаючи на те, що це може принести користь організаціям і програмістам, вони залишаються вразливими до хмарних загроз безпеки.

Більшість проблем, які були описані вище, є технічними. Проте, така проблема, як недостатня обачність, виникає, коли компанія має чітку стратегію щодо своїх цілей, ресурсів і рішень для хмарної системи безпеки. Іншими словами, це людський фактор. Крім того, поспішна міграція в комплексну хмарну інфраструктуру без належного планування можливості того, що послуги виправдають очікування споживачів, може поставити бізнес під загрозу проблем безпеки в хмарних обчисленнях. Це вкрай важливо для компаній, які

керують фінансовими даними клієнтів або чиї дані підпадають під дію таких нормативних актів, як FERPA, PCI, PCI-DSS та PII.

Поширеною проблемою є викрадення облікових записів. Це стало цілим набором нових випробувань через розширення та впровадження великою кількістю підприємств хмарних інструментів безпеки. Тепер зловмисники можуть віддалено отримувати доступ до конфіденційних даних, що зберігаються в хмарі, використовуючи дані для входу працівників. Вони навіть можуть змінювати та фальсифікувати їх, використовуючи облікові дані, які були викрадені. У 2023 році неправильно налаштований сегмент Amazon S3 відкрив особисті дані 119 мільйонів людей [53]. Того ж року зловмисник використав уразливість нульового дня, щоб викрасти облікові дані до хмарного постачальника ідентифікаційної інформації, що вплинуло на мільйони користувачів. Фішинг, клавіатурні логи та атаки переповнення буфера все ще є поширеними загрозами безпеці в хмарі. Однак, однією з найвизначніших нових загроз є атака «Людина в хмарі», під час якої зловмисники викрадають токени, які постачальники хмарних послуг використовують для перевірки окремих пристроїв, не вимагаючи входу під час кожного оновлення та синхронізації. Потім ці токени можуть дозволити несанкціонований доступ до хмарних облікових записів і даних.

Відповідно до звіту CSA [17], занепокоєння щодо ідентичності та доступу є першочерговим для професіоналів кібербезпеки. Проблеми доступу займають перше місце в списку, тому що захист даних починається й закінчується доступом. Віце-президент Forrester і головний аналітик Андраш Сер говорить: «Ідентифікація та доступ на платформах CSP — це все. Якщо у вас є ключі від королівства, ви не можете просто увійти в нього, а й змінити його конфігурацію — це серйозна загроза операційній стабільності та безпеці будь-якої організації». «Зловмисники більше не намагаються грубою силою проникнути в інфраструктуру підприємства», — додає Хенк Шлесс, старший менеджер із рішень безпеки в Lookout, постачальнику рішень для мобільного фішингу. «З такою кількістю способів компрометації та викрадення корпоративних

облікових даних краща тактика — видати себе за законного користувача, щоб уникнути виявлення». Оскільки все більше організацій переносять свої додатки в хмару, управління ідентифікацією залишається актуальною проблемою, стверджує Тушар Тамбей, віце-президент із розробки продуктів для рішень захисту даних у компанії Entrust, що займається цифровою безпекою та видачею облікових даних. «Оскільки багато компаній все ще працюють віддалено, IT-командам доводиться перевіряти особи співробітників, які працюють з будь-якого місця в будь-який час на будь-якому пристрої», — говорить він [54]. «Крім того, компанії взаємодіють із клієнтами та партнерами в хмарі». Тамбей додає, що управління ключами також має бути пріоритетним. «Надійне керування ключами може забезпечити безпеку даних і гарантувати, що довірені сторони матимуть доступ лише до тих даних, які є абсолютно необхідними», — каже він. «На жаль, захист даних за допомогою шифрування часто може викликати головний біль у управлінні ключами через зростаючу кількість ключів». Правильне керування ідентифікацією майже повністю залежить від користувача, каже Деніел Кеннеді, директор з досліджень інформаційної безпеки та мереж у 451 Research. «Хмарні постачальники надають допомогу, але гнучкість хмарних платформ вимагає ефективного керування доступом і привілеями користувачів і системи», — говорить він. - Це один із основних обов’язків підприємства, що використовує хмару в моделі спільної відповідальності, і тому займає важливе місце в оцінці ризику».

3.2. Технології контролю відповідності конфігурацій безпеки стандартам у хмарних середовищах

Постачальники хмарних обчислень досягли значних успіхів у забезпеченні відповідності безпеки різним стандартам. Ці платформи розроблено відповідно до суворих вимог, встановлених галузевими нормами, такими як Загальний регламент захисту даних (GDPR) і Закон про перенесення та підзвітність медичного страхування (HIPAA). Вони дотримуються

міжнародно визнаних стандартів, таких як ISO/IEC 27001 для систем управління інформаційною безпекою та SOC 2 для сервісних організацій.

Постачальники інвестують значні кошти в заходи безпеки для захисту даних клієнтів. Вони впроваджують надійні засоби контролю доступу, шифрування та протоколи безпеки мережі для захисту конфіденційної інформації. Крім того, більшість хмарних платформ проходять регулярні перевірки та оцінки безпеки, щоб підтвердити їх відповідність стандартам безпеки.

Організації, які використовують хмарні платформи, отримують переваги від вбудованих функцій безпеки та пропозицій відповідності, які надають ці постачальники. Це дозволяє компаніям зосередитися на своїй основній діяльності, одночасно використовуючи досвід і ресурси обраної хмарної платформи для забезпечення відповідності вимогам безпеки.

Під час вибору хмарної платформи організаціям важливо провести належну перевірку, щоб переконатися, що вона відповідає їхнім конкретним вимогам безпеки. Це може включати перевірку сертифікатів безпеки та аудиторських звітів, а також оцінку документації постачальника та процесів, пов’язаних із відповідністю.

Важливим критерієм при виборі постачальника є наявність у нього інструментів контролю відповідності стану безпеки хмари до міжнародних стандартів та норм. CSPM — це сегмент ринку для інструментів IT-безпеки, призначених для виявлення проблем із неправильною конфігурацією та ризиків відповідності в хмарі. CSPM допомагає постійно контролювати хмарну інфраструктуру на наявність прогалин у застосуванні політики безпеки.

Gartner ввів цей термін і описав CSPM як категорію продуктів безпеки, які допомагають автоматизувати безпеку та забезпечити відповідність у хмарі [55]. Інструменти CSPM вивчають і порівнюють хмарне середовище з певним набором передових практик і відомих ризиків безпеки. Деякі інструменти CSPM попереджають клієнтів, коли виникає необхідність усунути загрозу

безпеці, тоді як інші більш складні інструменти CSPM використовують роботизовану автоматизацію процесів для автоматичного усунення проблем.

CSPM використовується організаціями, які прийняли стратегію орієнтації на хмару та хочуть поширити свої найкращі методи безпеки на гібридні хмарні та багатохмарні середовища. Хоча CSPM часто асоціюється з IaaS, цю технологію також можна використовувати для мінімізації помилок конфігурації та зниження ризиків відповідності в середовищах SaaS і PaaS.

Більшість інструментів керування хмарною безпекою містять такі можливості:

Виявлення та видимість

CSPM забезпечує виявлення та видимість активів хмарної інфраструктури та конфігурацій безпеки. Користувачі можуть отримати доступ до єдиного джерела правди в багатохмарних середовищах і облікових записах. Хмарні ресурси та деталі виявляються автоматично після розгортання, включаючи неправильні конфігурації, метадані, мережу, безпеку та активність змін. Керування груповими політиками безпеки для облікових записів, регіонів, проектів і віртуальних мереж здійснюється через єдину консоль [56].

Управління та усунення неправильної конфігурації

CSPM усуває ризики безпеки та прискорює процес доставки шляхом порівняння конфігурацій хмарних додатків із галузевими та організаційними контрольними показниками, щоб можна було виявити та усунути порушення в режимі реального часу. Неправильні конфігурації, відкриті IP-порти, несанкціоновані модифікації та інші проблеми, які залишають хмарні ресурси відкритими, можна виправити за допомогою керованого виправлення, а також передбачено огорожі, щоб допомогти розробникам уникнути помилок. Зберігання контролюється, щоб належні дозволи завжди були на місці, і дані ніколи випадково не стали загальнодоступними. Крім того, екземпляри бази даних відстежуються, щоб забезпечити високу доступність, резервне копіювання та шифрування.

Постійне виявлення загроз

CSPM проактивно виявляє загрози протягом життєвого циклу розробки додатків, усуваючи шум попереджень безпеки багатохмарного середовища за допомогою цілеспрямованого підходу до виявлення загроз та керування ними. Кількість сповіщень зменшено, оскільки CSPM зосереджується на областях, які зловмисники, найімовірніше, використають, вразливості встановлюються за пріоритетом на основі середовища, а вразливий код не може досягти продуктивності. CSPM також буде постійно контролювати середовище на наявність зловмисної діяльності, неавторизованої діяльності та несанкціонованого доступу до хмарних ресурсів за допомогою виявлення загроз у реальному часі [57].

Інтеграція DevSecOps

CSPM зменшує витрати та усуває «тертя» та складність між мультихмарними постачальниками та обліковими записами. Вбудоване в хмару без агентне керування забезпечує централізовану видимість і контроль над усіма хмарними ресурсами. SOC та DevOps команди отримують єдине джерело правди, а групи безпеки можуть зупинити прогресування скомпрометованих активів протягом життєвого циклу програми.

Інструменти CSPM призначені для виявлення та усунення проблем, спричинених неправильною конфігурацією хмари. Проте деякі з них можуть використовувати лише визначені найкращі практики відповідно до певного хмарного середовища чи служби. Тому важливо знати, які інструменти можна використовувати в кожному конкретному середовищі. Наприклад, деякі інструменти можуть виявляти неправильні конфігурації лише в середовищі AWS або Azure. Деякі інструменти CSPM можуть автоматично виправляти проблеми, поєднуючи безперервний моніторинг у реальному часі з функціями автоматизації, які можуть виявляти та виправляти проблеми, наприклад неправильні дозволи облікового запису. Безперервну відповідність також можна налаштувати відповідно до кількох стандартів, зокрема HIPAA та інших, описаних у розділі 2.

3.3. Використання інструментів CSPM у хмарних середовищах

Вирішення проблем, пов’язаних із забезпеченням узгодженої відповідності галузевим стандартам, визначення пріоритетів і реагування на інциденти безпеки, а також підтримання єдиного уявлення про стан безпеки в різних облікових записах може бути особливо складним для підприємств, які працюють у хмарі. З великою кількістю постачальників, різними хмарними середовищами та загрозами, що постійно розвиваються, для організацій стає вкрай важливим мати комплексне рішення, яке може ефективно керувати їхніми потребами безпеки [24].

Одним із ключових аспектів такого рішення є можливість агрегувати інформацію про безпеку з різних джерел. Це включає збір даних від постачальників хмарних послуг, постачальників засобів безпеки та внутрішніх систем. Консолідуючи цю інформацію, організації можуть мати більш цілісне уявлення про загальний стан безпеки.

Однак одного лише збору даних недостатньо. Не менш важливо мати практичні висновки, отримані з цих даних. Комплексне рішення повинно мати можливість аналізувати зібрані дані та генерувати сповіщення або рекомендації на основі попередньо визначених правил або алгоритмів машинного навчання. Це допомагає командам безпеки визначати пріоритети та своєчасно й ефективно реагувати на виявлені факти безпеки.

Крім того, вкрай важливо підтримувати централізований контроль безпеки в різних хмарних облікових записах. Комплексне рішення має забезпечувати централізовану консоль керування, де можна визначати, розгортати та контролювати політики безпеки. Це дає змогу організаціям застосовувати узгоджені засоби контролю безпеки для всіх своїх хмарних облікових записів, незалежно від основного постачальника хмарних послуг [25].

Щоб забезпечити послідовну відповідність галузевим стандартам, рішення також має надавати можливість визначати та впроваджувати політики безпеки, які відповідають відповідним нормам і структурам. Це включає такі функції, як шаблони політики, набори правил, що настроюються, і автоматичне оцінювання відповідності [58]. Можливості регулярного сканування та створення звітів також необхідні для виявлення будь-яких прогалин у безпеці та забезпечення дотримання найкращих галузевих практик.

У цьому пункті показано процес застосування CSPM інструментів у найбільш популярних хмарних платформах: Amazon Web Service (AWS), Google Cloud Platform (GCP) та Microsoft Azure.

AWS Security Hub

Amazon Web Services (AWS) надає надійний набір інструментів і послуг, щоб допомогти організаціям захистити свої хмарні середовища. Серед них AWS Security Hub виділяється як потужний інструмент Cloud Security Posture Management (CSPM), який пропонує комплексну інформацію про безпеку та централізований контроль [18].

AWS Security Hub — це нативна служба AWS, яка діє як централізована інформаційна панель безпеки та відповідності. Вона об’єднує, упорядковує та ставить за пріоритетом результати безпеки з різних служб AWS, а також рішень безпеки AWS Partner Network (APN). Це дозволяє організаціям оптимізувати свої операції з безпеки, автоматизувати перевірки відповідності та швидко реагувати на потенційні загрози [21].

Ключові можливості:

1. Централізована інформаційна панель безпеки:

Security Hub збирає результати безпеки з таких служб AWS, як Amazon Guard Duty, AWS Config, AWS IAM Access Analyzer тощо. Він також інтегрується зі сторонніми інструментами безпеки, забезпечуючи повний огляд вашої безпеки.

2. Агрегація кількох облікових записів:

Центр безпеки дозволяє об’єднувати результати з кількох облікових записів AWS. Це особливо вигідно для великих підприємств або організацій зі складною інфраструктурою AWS.

3. Автоматичні перевірки відповідності:

Security Hub надає набір попередньо визначених стандартів відповідності, зокрема CIS AWS Foundations Benchmark, GDPR, HIPAA тощо. Він автоматично перевіряє ваші облікові записи на відповідність цим стандартам, спрощуючи керування відповідністю.

4. Спеціальна статистика та елементи керування:

Ви можете створити індивідуальні елементи керування безпекою та відповідністю відповідно до ваших конкретних вимог. Це дає вам змогу адаптувати стратегію безпеки відповідно до потреб вашої організації.

5. Пріоритетні результати безпеки:

Security Hub використовує систему підрахунку балів для визначення пріоритетності результатів безпеки. Це дає вам змогу спершу зосередитися на найважливіших проблемах, оптимізуючи зусилля з реагування.

6. Інтеграція з організаціями AWS:

Security Hub легко інтегрується з організаціями AWS, дозволяючи централізовано керувати налаштуваннями безпеки та відповідністю для всіх облікових записів учасників.

Увімкнувши AWS Security Hub, користувачі можуть обрати стандарт безпеки, який вони хочуть використовувати. Ці стандарти безпеки забезпечують набір елементів керування для визначення відповідності нормативним базам і найкращим галузевим практикам [59].

На даний момент клієнти мають змогу ввімкнути три автоматичні перевірки:

1. AWS Foundational Security Best Practices

Стандарт AWS Foundational Security Best Practices — це набір автоматизованих перевірок безпеки, які виявляють, коли облікові записи AWS і

розгорнуті ресурси не відповідають найкращим практикам безпеки. Стандарт визначено експертами з безпеки AWS. Цей підібраний набір елементів керування допомагає покращити вашу безпеку в AWS і охоплює найпопулярніші та базові служби AWS.

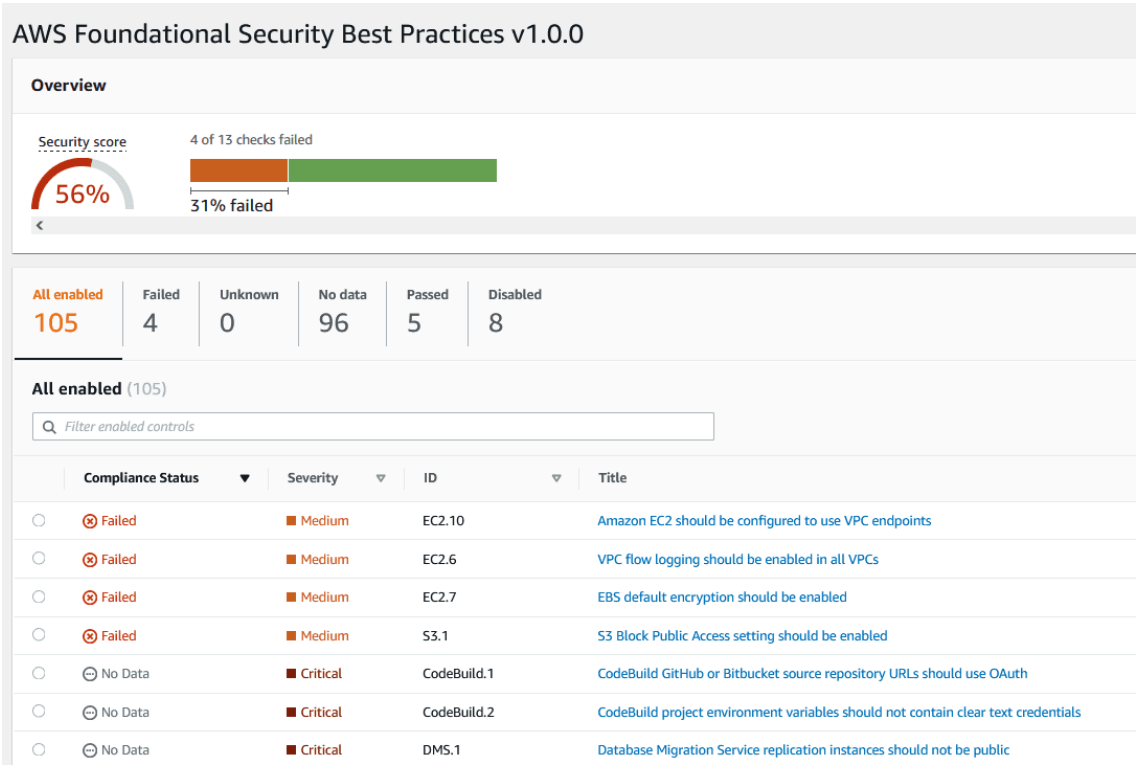

Рис. 3.1. AWS Foundational Security Best Practices [23]

2. AWS Security Hub CIS Benchmark

Центр безпеки в Інтернеті (CIS) опублікував тест із загальними рекомендаціями щодо безпеки для AWS. Цей стандарт Security Hub автоматично перевіряє готовність інфраструктури відповідати вимогам CIS.

Він включає такі речі, як:

- уникнення використання «root» облікового запису;
- перевірку того, що облікові дані, які не використовувалися протягом 90 днів або більше, вимкнено;
- переконання того, що політика паролів IAM вимагає мінімальної довжини символів 14 або більше;
- перевірка того, що MFA увімкнено для «кореневого» облікового запису;

- перевірка того, що жодна група безпеки не дозволяє вхід із 0.0.0.0/0 на порт 22;
- перевірка того, що ввімкнено ротацію створених клієнтом ключів KMS.

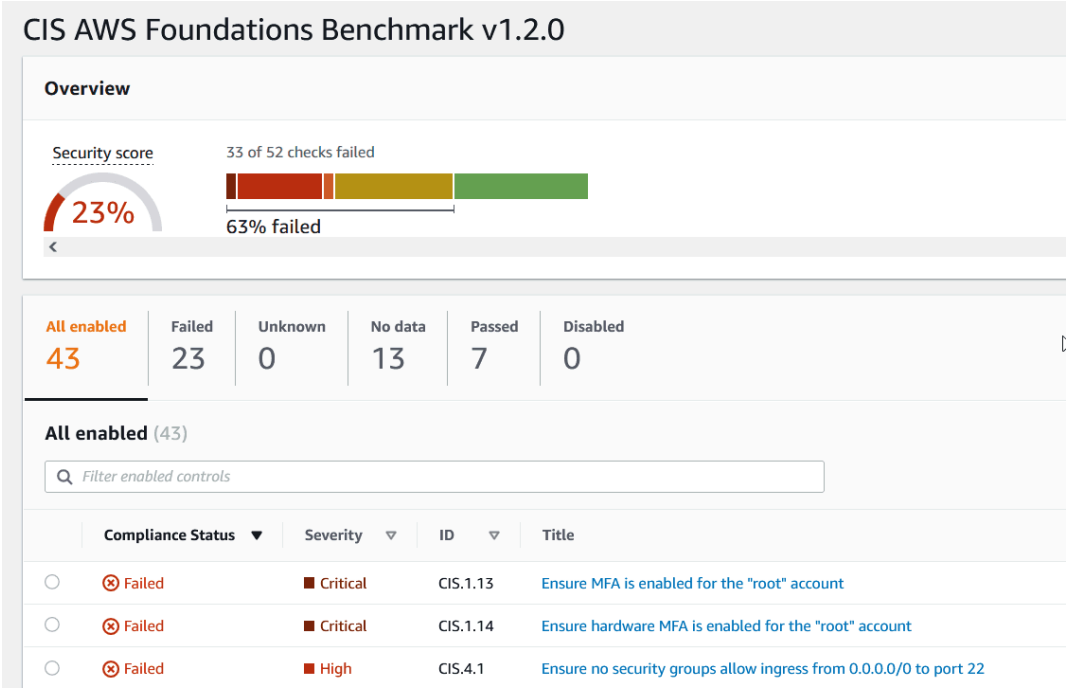

Рис. 3.2. AWS Security Hub CIS Benchmark [23]

3. Стандарт безпеки даних платіжних карток (PCI DSS)

Це набір перевірок, які стосуються платежів кредитними картками та стандартів, яких компанії повинні дотримуватися, якщо вони працюють з будь-якими справами, пов’язаними з кредитними картками.

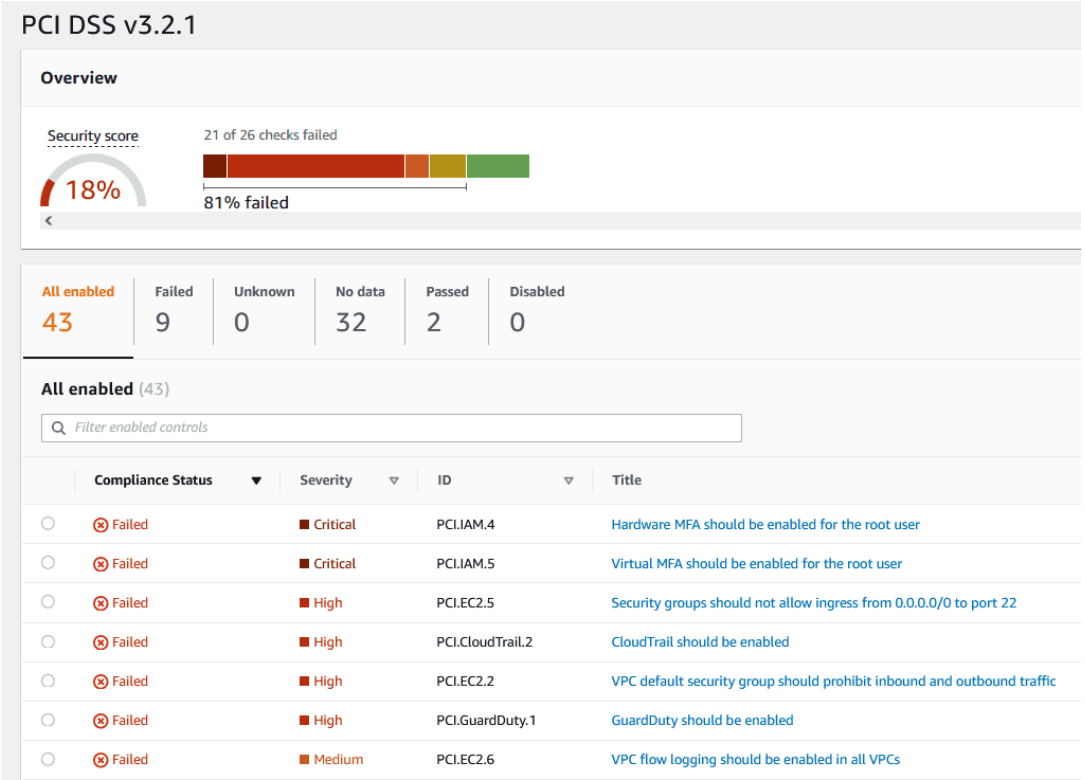

Рис. 3.3. PCI DSS [23]

GCP Security Command Center

Security Command Center допомагає посилити безпеку, оцінюючи ландшафт загроз та атак на дані; забезпечення інвентаризації та виявлення активів; виявлення неправильних конфігурацій, вразливостей і загроз; а також допомагає пом’якшити та усунути ризики.

Security Command Center використовує такі служби, як виявлення загроз і аналіз стану безпеки, щоб виявити проблеми безпеки у хмарному середовищі. Ці сервіси сканують логи та ресурси в Google Cloud, шукаючи індикатори загроз, вразливості програмного забезпечення та неправильні налаштування. Коли ці служби виявляють загрозу, вразливість або неправильну конфігурацію, вони видають висновок - це звіт або запис про окрему загрозу, вразливість або неправильну конфігурацію, яку служба виявила у середовищі Google Cloud. Результати показують виявлену проблему, ресурс Google Cloud, на який вона вплинула, і вказівки щодо вирішення проблеми [60].

У хмарній консолі Google Security Command Center надає консолідований перегляд усіх результатів, які повертаються службами Security Command Center. На консолі Google Cloud можна запитувати результати, фільтрувати їх, ігнорувати нерелевантні дані тощо.

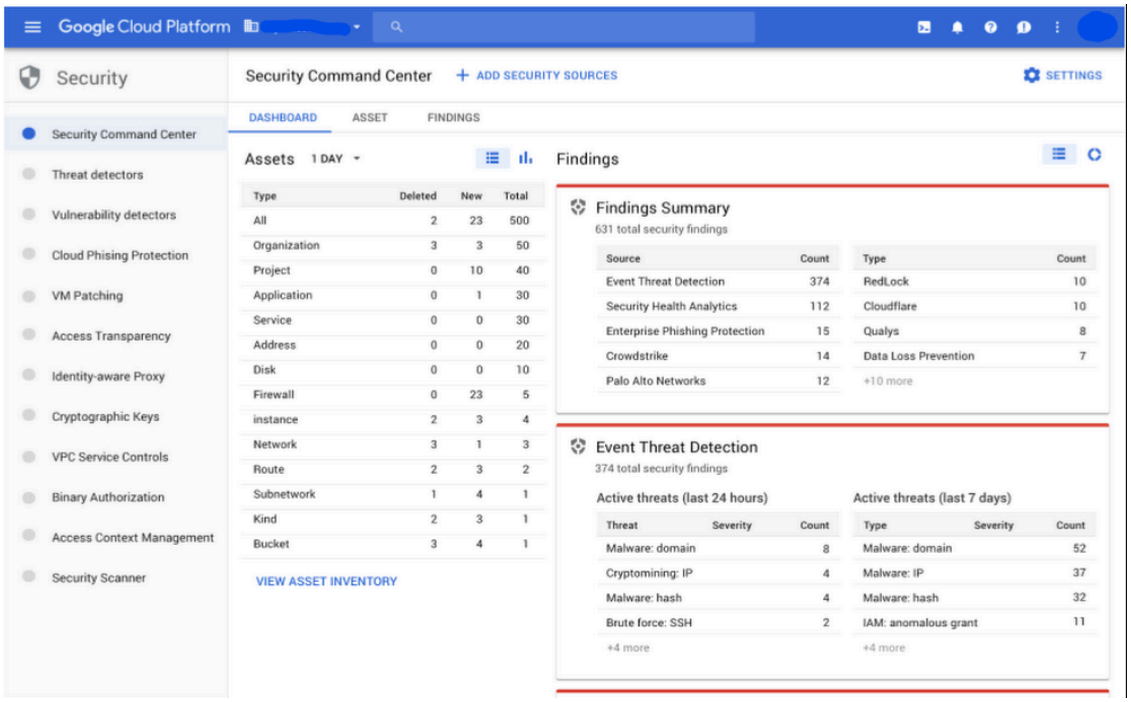

Рис. 3.4. GCP Security Command Center [19]

Виявлення загроз Google Security Command Center (SCC) є ключовим компонентом, спрямованим на захист хмарного середовища. Використовуючи складні алгоритми, SCC постійно шукає потенційні загрози безпеці, надаючи сповіщення в режимі реального часу та інформацію. SCC може виявляти неправильно налаштовані сегменти зберігання, які можуть ненавмисно оприлюднити конфіденційні дані, або відстежувати незвичайні призначення ролей IAM, які можуть збільшити привілеї понад налаштовані обмеження. Система також визначає потенційні вразливості веб-програм або сліди викрадення даних. Слідкуючи за такими ризиками безпеки, SCC відіграє ключову роль у забезпеченні того, щоб організації підтримували надійну безпеку в екосистемі Google Cloud.

Не менш важливим сервісом є Security Health Analytics (SHA) — це інструмент для підтримки працездатності та цілісності хмарних систем.

Завдяки комплексному моніторингу та аналізу він гарантує, що все функціонує належним чином різними способами:

- моніторинг стану безпеки: він постійно оцінює конфігурації безпеки та поведінку користувачів у різних хмарних службах;
- виявлення неправильних налаштувань: допомагає запобігти потенційним вразливостям. Однією з таких, яку SCC може виявити, є загальнодоступні місця зберігання даних. Бакети хмарного сховища, як-от у Google Cloud Storage, використовуються організаціями для зберігання великої кількості даних, починаючи від активів веб-сайтів і закінчуючи конфіденційними організаційними даними. За замовчуванням ці сегменти зберігання є приватними. Однак неправильні конфігурації іноді можуть зробити їх доступними для будь-кого, хто має посилання; вони навіть можуть стати загальнодоступними для пошуку, що потенційно може призвести до масових порушень даних. У минулому повідомлялося про численні випадки, коли компанії не навмисно залишали свої бакети для зберігання відкритими для громадськості, що призводило до розголошення конфіденційних даних, таких як відомості про клієнтів, внутрішні документи чи навіть резервні копії баз даних. Неправильні конфігурації хмарного сховища може бути ще важче виявити в багато хмарних середовищах;
- надання глибоких звітів: завдяки детальній аналітиці SCC пропонує практичну інформацію про наявну систему безпеки. Наприклад, його здатність автоматично створювати всеосяжні звіти про призначення ролей IAM може точно визначити аномалії, такі як член маркетингової команди, який несподівано отримує права адміністратора бази даних. Така інформація, незалежно від того, чи йдеться про простий недогляд, чи про потенційне порушення безпеки, підкреслює вміння SCC у проактивному виявленні ризиків і дозволяє організаціям оперативно виправляти проблеми та посилювати свої заходи безпеки;
- полегшення відповідності: SHA допомагає гарантувати, що хмарне середовище відповідає нормативним вимогам, спрощуючи керування

відповідністю. Більшість детекторів SCC відповідають таким стандартам, як CIS, PCI DSS, NIST 800-53, ISO 27001, OWASP TOP 10.

Azure Microsoft Defender

Microsoft Defender for Cloud (раніше відомий як Azure Security Center) — це комплексне рішення безпеки, яке забезпечує захист від загроз і керування безпекою для хмарних робочих навантажень і служб в Azure, а також локальних середовищ та інших хмарних платформ, як-от AWS і GCP. Це допомагає організаціям захистити їх хмарні робочі навантаження та сервіси від широкого спектру загроз та забезпечує необхідну видимість і контроль для ефективного керування безпекою.

За допомогою Microsoft Defender команди SOC можуть легко відстежувати та керувати станом безпеки, виявляти вразливі місця та розслідувати інциденти безпеки. Він забезпечує уніфіковану видимість і контроль у гібридних середовищах, дозволяючи командам безпеки легко керувати станом безпеки, і він інтегрується з іншими рішеннями безпеки Microsoft, такими як Azure Sentinel і Microsoft Cloud App Security, щоб забезпечити комплексне рішення безпеки для хмарних середовищ [61].

Інструмент використовує розширену аналітику та машинне навчання для виявлення та реагування на загрози в гібридних середовищах, включаючи віртуальні машини, контейнери, бази даних і безсерверні ресурси. Він допомагає організаціям захистити свої хмарні робочі навантаження та служби від широкого спектру загроз безпеці та забезпечує необхідну видимість і контроль для ефективного керування безпекою.

Ключовими можливостями Azure Microsoft Defender є:

- захист від загроз: Microsoft Defender надає розширені можливості захисту від загроз, які використовують штучний інтелект та машинне навчання для виявлення та блокування потенційних загроз у режимі реального часу. Він виявляє та блокує зловмисне програмне забезпечення, фішингові атаки та інші

форми кіберзагроз до того, як вони можуть завдати шкоди вашому хмарному середовищу;

- керування вразливими місцями: Microsoft Defender дає змогу виявляти та усувати вразливі місця у вашому хмарному середовищі, щоб зменшити ризик порушення безпеки. Він надає повне уявлення про стан безпеки вашої хмари та рекомендації щодо її покращення;
- управління відповідністю: інструмент допомагає дотримуватися нормативних стандартів, таких як HIPAA, GDPR і PCI DSS. Він забезпечує постійний моніторинг відповідності, автоматизовану оцінку відповідності та звітність про відповідність;
- керування ідентифікацією та доступом: сервіс надає можливості керування ідентифікацією та доступом, які дають змогу керувати доступом користувачів до вашого хмарного середовища. Він підтримує багатофакторну автентифікацію, умовний доступ і контроль доступу на основі ролей;
- аналіз загроз: Microsoft Defender надає можливості аналізу загроз, які дають змогу випереджати останні загрози безпеці. Він інтегрується з Центром аналізу загроз Microsoft для надання інформації про загрози та попереджень у реальному часі;
- керування інформацією про безпеку та подіями (SIEM): Microsoft Defender for Cloud інтегрується з такими рішеннями SIEM, як Azure Sentinel, Splunk і QRadar, щоб забезпечити централізований моніторинг безпеки, виявлення загроз і реагування на інциденти.

Сповіщення безпеки – це сповіщення або попередження, створені системами безпеки або програмним забезпеченням, щоб вказати, що було виявлено потенційну загрозу безпеці або проблему. Ці сповіщення призначені для сповіщення груп безпеки або адміністраторів про необхідність негайного вжиття заходів для розслідування потенційної загрози та реагування на неї.

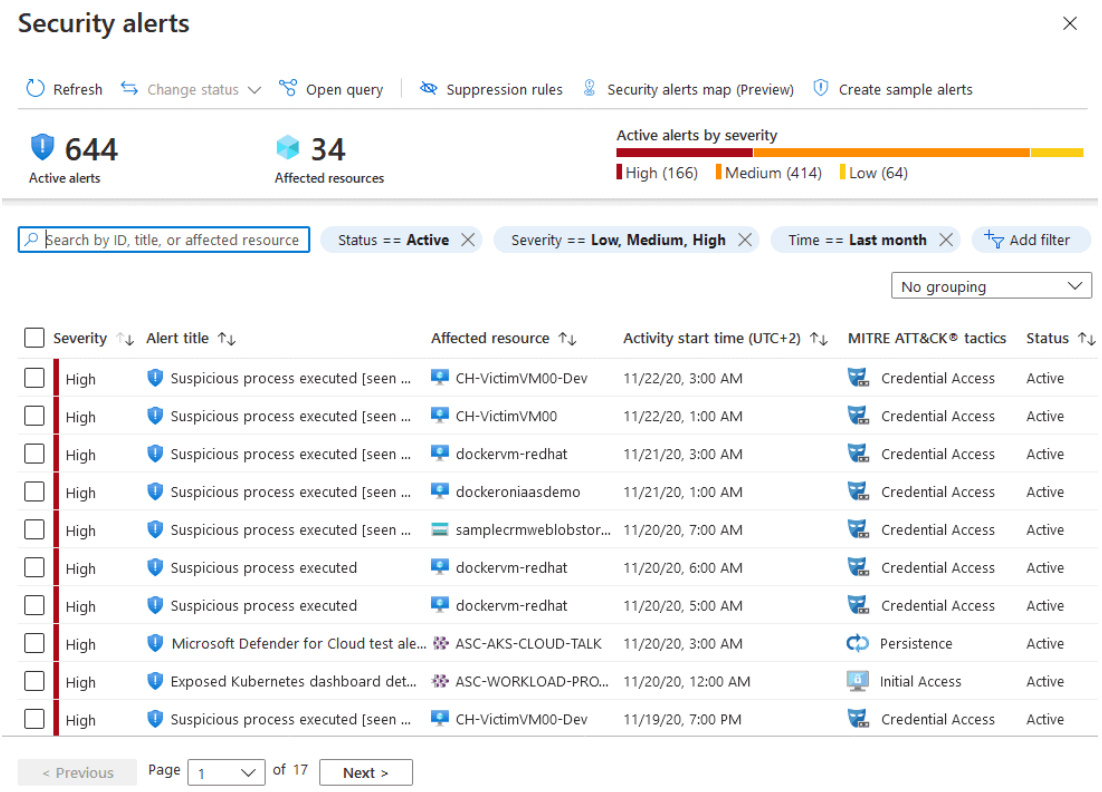

Рис. 3.5. Панель сповіщень безпеки Azure Microsoft Defender [20]

Висновки до третього розділу

Хоча хмарні обчислення є неймовірною можливістю для більшості підприємств гнучко реорганізувати свою інфраструктуру, правильне налаштування таких середовищ вимагає професійних знань та навичок. Як і більшість систем, хмарні середовища не позбавлені слабких місць. У цьому розділі було розглянуто ландшафт актуальних загроз безпеці хмар таких, як неправильна конфігурація та низький рівень контролю автентифікації. Важливо підкреслити, що хмарна безпека не надається за замовчуванням: її необхідно постійно підтримувати. Крім того, існує чимало вразливостей, якими може скористатися хакер, плануючи атаку. Адміністратори мережі повинні бути в курсі останніх подій щодо експлойтів сегментів S3 і бути дуже обережними щодо видалення резервних копій та інших даних. Лише вчасно враховуючи різні

хмарні ризики, можна створити безпечну модель, яка допоможе підприємствам досягати своїх цілей.

Щоб допомогти SOC командам утримувати актуальний стан безпеки відповідно до міжнародних стандартів та норм, існують технології контролю відповідності хмарних конфігурацій до цих стандартів. У розділі було розглянуто такі інструменти у популярних платформах хмарних обчислень: AWS, GCP та Azure. Також було показано ключові можливості цих сервісів та переваги їх використання.

ВИСНОВКИ

У кваліфікаційній роботі розв’язано актуальне наукове завдання особливостей застосування технологій контролю відповідності конфігурацій хмарних інфраструктур стандартам безпеки. Основні результати дослідження викладені у висновках, які зводяться до наступних положень:

1. Розкрито сутність технології хмарних обчислень, її структуру, шляхи використання, переваги та недоліки, а також важливість використання такого середовища сучасними компаніями.

2. Було виявлено, що незважаючи на продуманість технології, вона все одно не надає за замовчуванням засоби запоруки цілісності, конфіденційності та доступності даних. На сьогоднішній день хмарні середовища мають досить багато загроз та викликів, як, наприклад, неправильні конфігурації, витоки даних, відсутність контролю за привілеями користувачів.

3. Було проаналізовано питання важливості розробки заходів безпеки та їх відповідність профільним стандартам та регуляторним нормам. Впроваджуючи надійні практики та технології безпеки, організації можуть мінімізувати ймовірність людських помилок або ненавмисних порушень. Це включає використання надійних засобів контролю доступу, шифрування, регулярні оцінки безпеки та ретельний моніторинг для виявлення потенційних загроз і оперативного реагування на них.

4. Досліджено ландшафт актуальних загроз безпеці хмарних середовищ. Розуміння цих загроз та вжиття відповідних заходів безпеки дозволить забезпечити більш безпечні та надійні хмарні середовища.

5. Детально розглянуто стандарти та регуляторні норми у сфері безпеки хмарних середовищ. Орієнтуючись на них, компанії можуть бути впевнені, що безпека їх клієнтів на вищому рівні.

6. Проаналізовано інструменти, які допоможуть контролювати відповідність стану безпеки інфраструктури до вищезгаданих стандартів. Інструменти CSPM вивчають і порівнюють хмарне середовище з певним набором передових практик і відомих ризиків безпеки. CSPM використовується

організаціями, які прийняли стратегію орієнтації на хмару та хочуть поширити їх найкращі методи безпеки на гібридні хмарні та багатохмарні середовища.

ПЕРЕЛІК ПОСИЛАНЬ

1. Types of cloud computing. URL: https://aws.amazon.com/types-of-cloud-computing/

2. Infrastructure as a Service (IaaS) in Cloud Computing. URL: https://www.mongodb.com/cloud-explained/iaas-infrastructure-as-a-service

3. SaaS vs PaaS vs IaaS and More: Cloud Service Models Compared. URL: https://geekflare.com/cloud-service-models/

4. What is the Software As A Service business model. URL: https://www.servissoft.net/en/what-is-saas-sector-news/

5. 12 Benefits of Cloud Computing. URL: https://www.salesforce.com/products/platform/best-practices/benefits-of-cloud-computing/

6. SolarWinds hack explained: Everything you need to know. URL: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know/

7. T-Mobile Data Leak Report. URL: https://www.sec.gov/ix?doc=/Archives/edgar/data/0001283699/000119312523010949/d641142d8k.htm/

8. Choose Adaptive Data Governance Over One-Size-Fits-All for Greater Flexibility. URL: https://www.gartner.com/en/articles/choose-adaptive-data-governance-over-one-size-fits-all-for-greater-flexibility/

9. AWS Compliance to National Institute of Standards and Technology. URL: https://aws.amazon.com/compliance/nist/

10. Azure and NIST Cybersecurity Framework. URL: https://learn.microsoft.com/en-us/azure/compliance/offerings/offering-nist-csf/

11. ISO/IEC 27017 Cloud Security Controls. URL: https://www.isms.online/iso-27017/

12. Cloud Security Standards. URL: https://www.geeksforgeeks.org/cloud-security-standards/

13. AWS CIS Controls v7.1 Implementation Group 1. URL: https://docs.aws.amazon.com/audit-manager/latest/userguide/CIS-controls.html

14. What is a HIPAA Compliant Cloud Drive? URL: https://www.hipaajournal.com/hipaa-compliant-cloud-drive/

15. What are your biggest cloud security concerns? URL: https://www.statista.com/statistics/1172265/biggest-cloud-security-concerns-in-2020/

16. Te-Shun Chou. Security Threats on Cloud Computing Vulnerabilities. URL: https://www.researchgate.net/publication/289756317_Security_Threats_on_Cloud_Computing_Vulnerabilities

17. 11 top cloud security threats. URL: https://www.csoonline.com/article/555213/top-cloud-security-threats.html

18. Anshoo Verma. Comprehensive Cloud Security with AWS CSPM Native Service: Security Hub. URL: https://medium.com/@anshooverma/comprehensive-cloud-security-with-aws-cspm-native-service-security-hub-d5e745ce3f72

19. Prasanna Bhaskaran Surendran. Security Command Center-Google Cloud. URL: https://medium.com/google-cloud/security-command-center-google-cloud-b9872263b6a0

20. Ajay Kumar. Microsoft Defender Cloud Security Posture Management (CSPM) — A Pillar for Multi Cloud Security Management. URL: https://intouchajay.medium.com/microsoft-defender-cloud-security-posture-management-cspm-a-pillar-for-multi-cloud-security-f0f7809247

21. What is AWS Security Hub? Definition, Benefits & Pricing. URL: https://www.stormit.cloud/blog/aws-security-hub/

22. What is cloud security? URL: https://www.ibm.com/topics/cloud-security

23. What is AWS Security Hub? URL: https://docs.aws.amazon.com/securityhub/latest/userguide/what-is-securityhub.html

24. Cloud Security Posture Management: Why You Need It Now. URL: https://cloudsecurityalliance.org/blog/2019/10/01/cloud-security-posture-management-why-you-need-it-now/

25. What is cloud security posture management (CSPM)? URL: https://www.cloudflare.com/en-gb/learning/cloud/what-is-cspm/

26. What is the cloud? Cloud definition. URL: https://www.cloudflare.com/en-gb/learning/cloud/what-is-the-cloud/

27. What are Iaas, Paas and Saas? URL: https://www.ibm.com/topics/iaas-paas-saas

28. Atul Kumar. Top 3 Cloud Computing Service Models: SaaS/PaaS/IaaS. URL: https://k21academy.com/amazon-web-services/aws-solutions-architect/cloud-service-models/

29. Cloud Servie Models. URL: https://www.guru99.com/cloud-service-models.html

30. Widespread Adoption of Cloud Computing and Modern Development Technologies Will Have a Dramatic Impact on the Composition of IT Teams. URL: https://www.idc.com/getdoc.jsp?containerId=prUS50792523

31. 13 Key Cloud Computing Benefits for Your Business. URL: https://www.globaldots.com/resources/blog/cloud-computing-benefits-for-your-business/

32. Advantages and disadvantages of the cloud. URL: https://www.kio.tech/en-us/blog/nube/advantages-and-disadvantages-of-the-cloud

33. 6 Explosive Cloud Facts. URL: https://rapidscale.net/resources/blog/managed-cloud-services/6-explosive-cloud-facts

34. Cloud Security: Principles, Solutions, and Architectures. URL: https://www.exabeam.com/explainers/cloud-security/cloud-security-principles-solutions-and-architectures/

35. Analysis of Approaches to Ensure the Security of Cloud Services. URL: https://boostylabs.com/approaches-to-ensure-security-of-cloud-services

36. Cloud Assets The Biggest Targets For Cyberattacks, As Data Breaches Increase. URL: https://www.thalesgroup.com/en/worldwide/security/press_release/cloud-assets-biggest-targets-cyberattacks-data-breaches-increase

37. Sharon Shea. Top 11 cloud security challenges and how to combat them. URL: https://www.techtarget.com/searchsecurity/tip/Top-11-cloud-security-challenges-and-how-to-combat-them

38. Cloud Security Issues & Challenges. URL: https://www.kaspersky.com/resource-center/preemptive-safety/cloud-security-issues-challenges

39. Security Issues in Cloud Computing. URL: https://www.geeksforgeeks.org/security-issues-in-cloud-computing/

40. Navigating Cloud Security Challenges: Top concerns for Businesses in 2023. URL: https://www.visionet.com/blog/navigating-cloud-security-challenges

41. Deepak Gupta. Cloud Security Challenges Today: Expert Advice on Keeping your Business Safe. URL: https://www.loginradius.com/blog/identity/cloud-computing-security-challenges/

42. Kathleen Casey. What is Shadow IT? URL: https://www.techtarget.com/searchcloudcomputing/definition/shadow-IT-shadow-information-technology

43. Tally Shea. How to Perform a Cloud Risk Assessment. URL: https://sonraisecurity.com/blog/how-to-perform-a-cloud-risk-assessment/

44. Raj Pathak. The Crucial Role of Identity and Access Management (IAM) in Cloud Security. URL: https://www.linkedin.com/pulse/crucial-role-identity-access-management-iam-cloud-security-raj-pathak

45. Shared responsibility in the cloud. URL: https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

46. General Data Protection Regulation. URL : https://gdpr-info.eu/

47. Health Insurance Portability and Accountability Act of 1996 (HIPAA). URL: https://www.cdc.gov/phlp/publications/topic/hipaa.html

48. What are the key cloud security standards and frameworks to follow? URL: https://www.linkedin.com/advice/0/what-key-cloud-security-standards-frameworks

49. NIST Special Publication 800-53. URL: https://www.nist.gov/privacy-framework/nist-sp-800-53

50. Robert Sheldon. What is SOC 2? URL: https://www.techtarget.com/searchsecurity/definition/Soc-2-Service-Organization-Control-2

51. Cloud security threats, risks and vulnerabilities. URL: https://nordlayer.com/learn/cloud-security/risks-and-threats/

52. Mahendra D. Top 15 Cloud Security Vulnerabilities. URL: https://www.pingsafe.com/blog/cloud-security-vulnerabilities/

53. Nivedita James Palatty. Cloud Vulnerability Management: The Detailed Guide. URL: https://www.getastra.com/blog/security-audit/cloud-vulnerability-management/

54. Top 10 Cloud Attacks and What You Can Do About Them. URL: https://www.aquasec.com/cloud-native-academy/cloud-attacks/cloud-attacks/

55. Cloud Security Posture Management. URL: https://www.gartner.com/en/information-technology/glossary/cloud-security-posture-management

56. What is CSPM? URL: https://www.microsoft.com/en-us/security/business/security-101/what-is-cspm

57. Cloud Security Posture Management Explained. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-cloud-security-posture-management

58. The Need for Cloud Security Posture Management. URL: https://www.exabeam.com/explainers/cloud-security/what-is-cloud-security-posture-management-cspm/

59. Five Signs Your Organization Needs AWS Security Hub. URL: https://www.infopulse.com/blog/why-use-aws-security-hub

60. Alexander Hose. How To Secure Your Cloud With GCP Security Command Center. URL: https://alexanderhose.com/how-to-secure-your-cloud-with-gcp-security-command-center/

61. Review cloud security posture. URL: https://learn.microsoft.com/en-us/azure/defender-for-cloud/overview-page