ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія управління ідентифікацією та доступом клієнтів за допомогою Akamai Identity Cloud»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

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

_____ Олександр КОМПАНЕЦЬ
(підпис)

Виконав: здобувач(ка) вищої освіти групи БСДМ-63
КОМПАНЕЦЬ Олександр
(прізвище, ім'я)

Керівник д.ф. СОБЧУК Андрій
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2024

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПК – персональний комп’ютер

ЦОД – центр обробки даних

API – Application Programming Interface

APT – Advanced Persistent Threat

CIAM – Customer Identity and Access Management

CNAPP – Cloud-Native Application Protection Platform

CSP – Credential Service Provider

DDoS – Distributed Denial of Service

DNS – Domain Name System

IaaS – Infrastructure as a Service

IAL – Identity Assurance Level

IAM – Identity and Access Management

MFA – Multi-Factor Authentication

MSSP – Managed Security Service Provider

OWASP – Open Web Application Security Project

RP – Relying Partie

SAML – Security Assertion Markup Language

SOC – Security Operations Center

SSO – Single Sign-On

WAAP – Web Application and API protection

WAF – Web Application Firewall

ВСТУП

Актуальність дослідження. Організації використовують рішення ідентифікації клієнтів і керування доступом, щоб контролювати доступ до загальнодоступних веб-сайтів і цифрових ресурсів. Рішення управління ідентифікацією та доступом до хмарних сервісів полегшують клієнтам реєстрацію та вхід у онлайн-додатки та сервіси. Вони допомагають забезпечити конфіденційність даних і захистити від крадіжки особистих даних та інших видів шахрайства та зловживань. Рішення управління ідентифікацією та доступом до хмарних сервісів дозволяють клієнтам легко керувати своїми профілями облікових записів і налаштуваннями безпеки самостійно.

Рішення управління ідентифікацією та доступом до хмарних сервісів спрощують для організацій додавання функцій реєстрації користувачів і надійного керування їх ідентифікацією та контролю доступу до додатків, орієнтованих на клієнтів. Вони допомагають організаціям покращити взаємодію з клієнтами, посилити безпеку та покращити дотримання вимог конфіденційності даних, таких як GDPR. Рішення управління ідентифікацією та доступом до хмарних сервісів зазвичай надаються як хмарні служби, які розміщуються та керуються надійною третьою стороною для максимальної простоти, гнучкості та масштабованості.

Вищесказане визначає актуальність теми даної кваліфікаційної роботи, основний зміст якої становлять дослідження технології управління ідентифікацією та доступом клієнтів до хмарних сервісів організації на базі Akamai Identity Cloud.

Об'єкт дослідження – управління ідентифікацією та доступом клієнтів до хмарних сервісів організацій.

Предмет дослідження – технологія управління ідентифікацією та доступом клієнтів до хмарних сервісів організації на базі Akamai Identity Cloud.

Мета роботи – розробити порядок застосування технології управління

ідентифікацією та доступом клієнтів до хмарних сервісів організації та рекомендації щодо її реалізації.

Наукові завдання:

дослідити сутність проблеми управління ідентифікацією та доступом клієнтів до хмарних сервісів організацій;

проаналізувати підходи до управління ідентифікацією та доступом клієнтів до хмарних сервісів організацій;

проаналізувати існуючі рішення для управління ідентифікацією та доступом клієнтів до хмарних сервісів організацій;

проаналізувати методи та засоби управління ідентифікацією та доступом клієнтів до хмарних сервісів організації на базі Akamai Identity Cloud;

розкрити порядок реалізації технології управління ідентифікацією та доступом клієнтів до хмарних сервісів організації на базі Akamai Identity Cloud.

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

Практичне значення одержаних результатів: запропоновано порядок застосування технології управління ідентифікацією та доступом клієнтів до хмарних сервісів організації на базі Akamai Identity Cloud, а також розроблено рекомендації фахівцям з кібербезпеки щодо її реалізації.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 25 жовтня 2024 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ТА ДОСТУПОМ КЛІЄНТІВ ДО ХМАРНИХ СЕРВІСІВ ОРГАНІЗАЦІЙ

1.1. Дослідження проблеми управління ідентифікацією та доступом клієнтів до хмарних сервісів організацій

У Звіті Imperva [1] зазначається, що атаки захоплення облікового запису є одними з найпоширеніших автоматичних загроз. Вони передбачають використання ботів для спроб несанкціонованого доступу та захоплення облікових записів користувачів за допомогою методів підміни облікових даних і злому, що призводить до крадіжки цифрових даних і значних збитків для організацій. Згідно з даними Aite Group, збитки від крадіжки особистих даних у 2023 році сягнуть 635,4 мільярдів доларів [1]. На рисунку 1.1 представлені статистичні дані про щомісячні атаки захоплення облікового запису, зафіксовані Imperva за останні два роки.

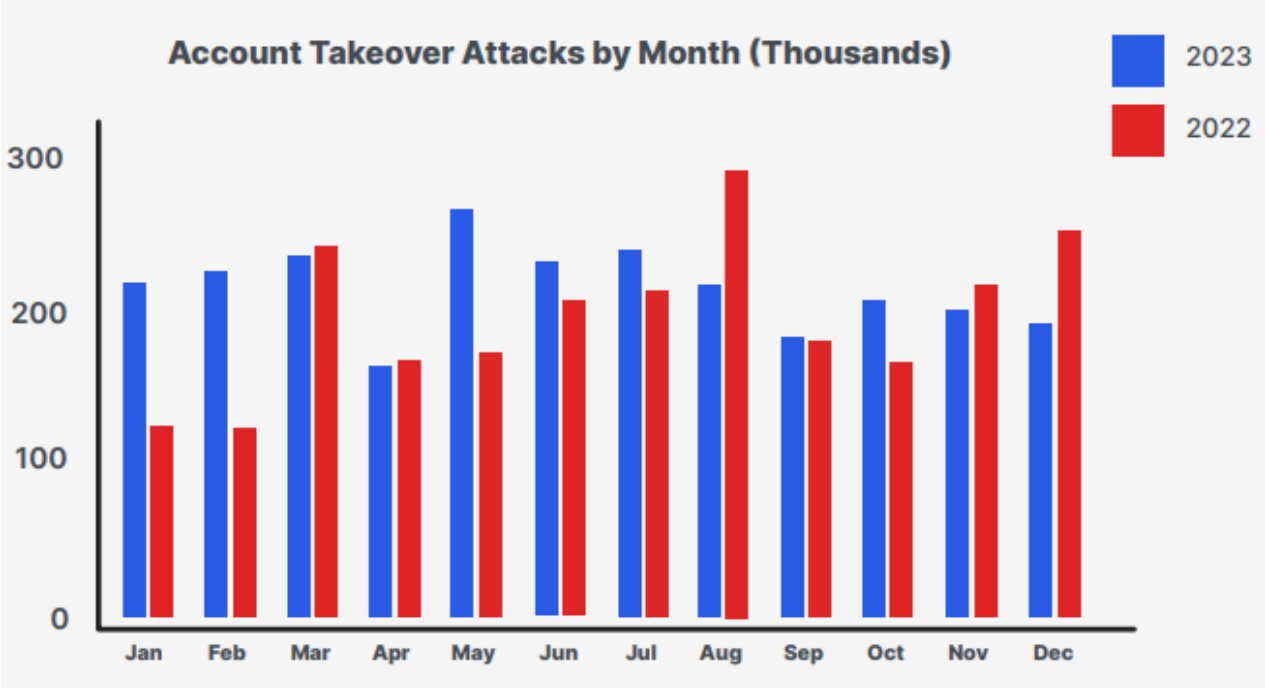

Рис. 1.1. Статистика щомісячних атак захоплення облікового запису, зафіксовані Imperva [1]

В багатохмарних середовищах існують критичні точки, через які проходить більшість мережевого трафіку. У разі зламу ці точки дозволяють зловмисникам розгалужуватися та отримувати доступ до більшої кількості ресурсів у вашій мережі. На рисунку 1.2 показано кілька шляхів атаки, що походять із загальнодоступного Інтернету.

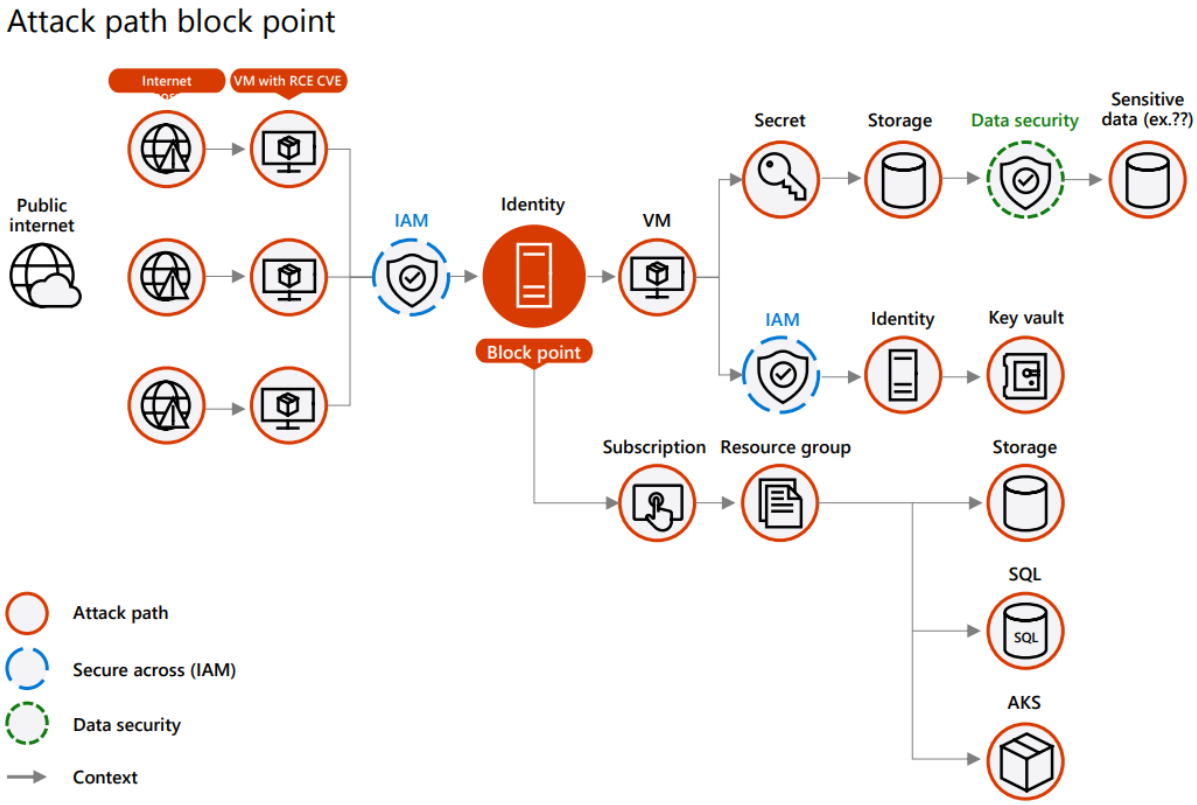

Рис. 1.2. Основні шляхи атак, що походять із загальнодоступного Інтернету [10]

У цьому прикладі є три віртуальні машини (VM) із CVE віддаленого виконання коду (RCE). Зловмисники можуть скористатися цими CVE, щоб отримати доступ до ідентифікаційної інформації, закріпитися у вашому середовищі та переміститися в бік, щоб отримати доступ до конфіденційних даних, сховища ключів або кластера AKS. Зловмисники можуть націлюватися на всі ці потенційні шляхи атаки, навіть вирішуючи переслідувати один шлях атаки за раз, щоб у разі виявлення на одному шляху вони могли змінити свою стратегію та зберегти опору в середовищі. Організації можуть захистити ці точки блокування, впровадивши CNAPP, щоб запобігти просуванню зловмисників по

шляху атаки.

Microsoft [10] визначає ідентифікацію та керування доступом користувачів до хмарних сервісів основним елементом хмарної безпеки. Групи безпеки мають не лише відстежувати та захищати ідентифікаційні дані користувачів, але й враховувати ідентифікаційні дані робочого навантаження. Це особливо складно, враховуючи те, як швидко зростали ідентифікаційні дані та їхній доступ до хмарних ресурсів за останні роки, коли все більше і більше робочих ідентифікаційних осіб отримують доступ до хмарних ресурсів. Ідентичності робочого навантаження зараз перевищують кількість ідентичностей людей, і цей розрив лише зростає.

Захист ідентифікаторів робочого навантаження є надзвичайно важливим. Оскільки все більше компаній переносять свої робочі навантаження в хмару, ми спостерігаємо швидке зростання кількості створюваних ідентифікаторів робочого навантаження. Сьогодні існує одна людина на кожні 10 ідентифікацій робочого навантаження. Ця проблема є ще гострішою серед малих і середніх підприємств, які мають одну ідентифікаційну інформацію людини на кожні 50 ідентифікаційних даних робочого навантаження. З 209 мільйонів ідентифікаційних даних, які Microsoft Entra Permissions Management виявила в хмарах своїх клієнтів у 2023 році (рисунок 1.3).

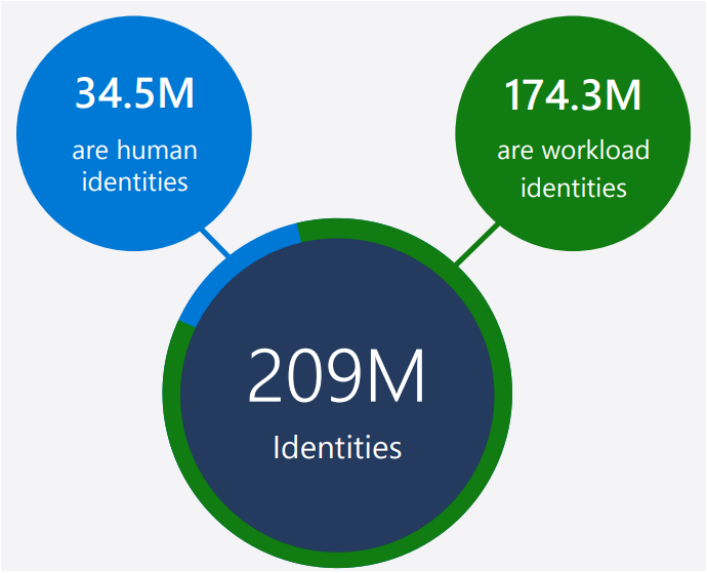

Рис. 1.3. Кількість ідентифікаційних даних, які Microsoft Entra Permissions Management виявила в хмарах своїх клієнтів у 2023 році [10]

Оскільки кількість ідентифікацій робочого навантаження продовжує значно перевищувати кількість ідентифікаторів людей, важливо враховувати відносний ризик кожного з них. Менша кількість рішень може належним чином захистити особисті дані робочого навантаження порівняно з тим, як ці рішення можуть захистити та захистити особисті дані людей. Це пояснюється тим, що більшість рішень ідентифікації та доступу на сьогоднішньому ринку зосереджено на захисті ідентифікаційних даних людей, а не ідентифікаційних даних робочого навантаження [10].

Ідентифікатори робочого навантаження також набагато складніше захистити, ніж ідентифікатори людини, оскільки вони не мають чітко визначеного життєвого циклу. Коли новий співробітник або сторонній підрядник приєднується до вашої компанії, вони мають чітко визначену дату початку, яка часто супроводжується кадровими та іншими пов’язаними процесами. Коли їхня взаємодія з вашою організацією закінчується – чи то через те, що вони перейшли на нову роботу, чи через те, що їхній контракт закінчився – ця кінцева дата також чітко зазначається в багатьох системах компанії. Однак це не стосується ідентифікацій робочого навантаження, які можуть поступово звужуватися та ставати неактивними. Це особливо вірно, якщо врахувати широке використання тіньових IT у багатохмарних середовищах. Неактивні ідентифікаційні дані контролюються не так само, як активні ідентифікаційні дані, що робить їх привабливою мішенню для зловмисників для компрометації, оскільки вони можуть використовувати ідентифікаційні дані або облікові дані для переміщення в бік у вашому середовищі. Ідентифікатори робочого навантаження також можна вручну вставляти в код, що ускладнює їх очищення без небажаних наслідків [10].

Підприємства використовують рішення ідентифікації клієнтів і керування доступом (Customer Identity and Access Management, CIAM), щоб контролювати доступ до загальнодоступних веб-сайтів і цифрових ресурсів. Рішення CIAM полегшують клієнтам реєстрацію та вхід у онлайн-додатки та служби. Вони допомагають захистити конфіденційність даних і захистити від крадіжки особистих даних та інших видів шахрайства та зловживань. І вони дозволяють

клієнтам легко керувати своїми профілями облікових записів і налаштуваннями безпеки самостійно [2].

Рішення CIAM спрощують для компаній додавання функцій реєстрації користувачів і надійного керування ідентифікацією та контролю доступу до корпоративних додатків, орієнтованих на клієнтів. Вони допомагають компаніям покращити взаємодію з клієнтами, посилити безпеку та дотриматися вимог щодо конфіденційності даних, таких як GDPR [2].

Рішення CIAM зазвичай надаються як хмарні служби, які розміщуються та керуються надійною третьою стороною для максимальної простоти, гнучкості та масштабованості. Необхідно підкреслити, що збираючи та обробляючи дані клієнтів, організації повинні дотримуватися багатьох правил захисту даних і конфіденційності. Рішення для керування ідентифікацією, наприклад Akamai Identity Cloud, може допомогти впоратися з цими проблемами.

Розглянемо проблеми при впровадженні технології ідентифікації клієнта та керування доступом (CIAM) [5].

1. Інтеграція з існуючими системами: більшість організацій залишаються на старих системах, які можуть погано інтегруватися з рішеннями CIAM, які зараз є на ринку. Інтеграція CIAM із такими системами може зайняти багато часу, грошей і ресурсів, щоб зробити інтеграцію ідеальною. Це пов’язано з тим, що рішення CIAM, які розгортають організації, які мають складну та різноманітну технологічну інфраструктуру, складно інтегрувати, тестувати та працювати з високим ступенем взаємозв’язку між різними платформами, програмами та середовищами, які складають технологічну екосистему підприємства.

2. Безпека даних і конфіденційність: рішення CIAM працюють з персональними даними клієнтів, що робить рішення потенційно вразливими до кіберзагроз. Одним із головних питань є забезпечення ефективних заходів захисту даних, а також підготовка реагування на випадки витоку даних. У середовищі, що постійно змінюється, може бути складно обробляти та захищати дані клієнта таким чином, щоб повністю поважати конфіденційність і відповідати положенням про згоду.

3. Підтвердження особи користувача: точна й ефективна перевірка автентичності ідентифікаційних даних користувачів є складною справою, особливо в середовищах із великою кількістю реєстрацій нових користувачів. Впровадження ефективних стратегій виявлення та пом’якшення шахрайства має вирішальне значення для захисту від крадіжки особистих даних та інших зловмисних дій.

4. Управління витратами та ресурсами: впровадження рішень CIAM може бути дорогим, головним чином через те, що рішення передбачає значні інвестиції в технології, інтеграцію та обслуговування. Іншою актуальною проблемою є відсутність належного людського та фінансового капіталу для підтримки впровадження та підтримки систем CIAM.

5. Керування кількома ідентифікаторами: бувають випадки, коли організації доводиться мати справу з тим самим користувачем у багатьох системах і програмах з різними ролями та дозволами. Тому непросто досягти послідовної та консолідованої стратегії в управлінні ідентифікацією. Важко й важливо розвинути повну перспективу кожного клієнта шляхом консолідації інформації з численних джерел з метою надання індивідуальних зустрічей і задовільного обслуговування.

6. Технологічна складність: через швидкий і невпинний розвиток технологій рішення CIAM потрібно повільно оновлювати, щоб вони відповідали новим загрозам безпеці, вимогам користувачів і нормативам. Впровадження та обслуговування CIAM передбачає використання технічного персоналу, який може виявитися дефіцитним і дорогим.

1.2. Аналіз підходів до управління ідентифікацією та доступом клієнтів до хмарних сервісів організацій

Рішення Customer Identity and Access Management (CIAM) пропонують набір можливостей для безпечного й ефективного керування ідентифікацією клієнтів і доступом. Основні функції включають реєстрацію користувача, автентифікацію, авторизацію, єдиний вхід (SSO), багатофакторну автентифікацію (MFA),

перевірку ідентифікації, керування згодою та налаштуваннями та керування профілями користувачів.

Порівнюючи CIAM і IAM, важливо відзначити, що перший зосереджений на клієнтах, а другий – на користувачах. Хоча IAM здебільшого зосереджено на ідентифікації внутрішніх користувачів організації та їхньому доступі до доступних ресурсів, CIAM спеціально розроблено для задоволення потреб зовнішніх клієнтів або споживачів компанії. Перше призводить до різних цілей, атрибутів і факторів для кожного виду управління ідентифікацією [6].

Ідентифікація клієнта та керування доступом:

Методи автентифікації: CIAM використовує багатофакторну автентифікацію (MFA), можливості входу через соціальні мережі та біометричну ідентифікацію. Ці методи покращують безпеку, оскільки надають користувачеві гнучкість і зручність.

Інтеграція: CIAM працює в поєднанні з додатками для клієнтів, такими як електронна комерція, портали та мобільні додатки. Це спосіб переконатися, що користувачі мають знайому та безпечну точку контакту з організацією на всьому протязі.

Управління життєвим циклом: CIAM відповідає за створення шляху клієнта від залучення до активації та лояльності. Завдяки цьому користувач отримує гарний і безпечний досвід під час роботи з компанією.

Персоналізація: CIAM має широкі можливості налаштування, які адаптують рішення до звичок або вибору користувача. Це допомагає надавати вміст і рекомендації, які мають відношення до клієнта, таким чином покращуючи досвід клієнтів.

Керування ідентифікацією та доступом:

IAM є важливим компонентом сучасної кібербезпеки, який охоплює політики, технології та процеси для визначення та адміністрування цифрових ідентифікацій і прав доступу в організаціях, захисту конфіденційних даних і застосування нормативних вимог, а також оптимізації доступу користувачів.

Методи автентифікації: IAM використовує надійні методи автентифікації,

такі як багатофакторна автентифікація (MFA), смарт-картки, біометричні дані та токени. Ці методи гарантують, що внутрішній доступ захищено на найвищому рівні.

Інтеграція: IAM взаємодіє з іншими системами компанії, включаючи системи управління персоналом, внутрішні програми та інші організаційні ресурси. Ця інтеграція також допомагає централізувати контроль доступу.

Управління життєвим циклом. Управління працівниками починається і закінчується IAM, від моменту прийняття працівника на роботу до моменту його/її звільнення з компанії.

Персоналізація: IAM забезпечує скромний рівень персоналізації, оскільки він більше стосується стандартного доступу та політик. Метою є досягнення однакового та безпечного доступу в усій організації відповідно до організаційних посад та обов'язків.

Основні можливості ідентифікації клієнта та керування доступом (CIAM)

Реєстрація клієнтів і адаптація: рішення CIAM пропонують плавні та легко адаптовані методи реєстрації, такі як електронна пошта, обліковий запис у соціальних мережах або система єдиного входу. Це скорочує витрати та збільшує шанси споживачів прийняти системи.

Керування обліковим записом самообслуговування: портали самообслуговування дозволяють контролювати особистий обліковий запис, змінювати персональні дані та налаштовувати налаштування користувачами. Це корисно для користувачів і звільняє багато організацій від виконання багатьох складних процедур.

Багатофакторна автентифікація (MFA): MFA робить облікові записи більш безпечними, оскільки людям пропонується ввести два або більше факторів, перш ніж отримати доступ до облікового запису. Це може бути щось, що людина знає, як-от пароль, те, що в неї є, як-от мобільний пристрій, або навіть те, що є біометричним.

Єдиний вхід (SSO): SSO означає єдиний вхід; тут користувачеві потрібно лише один раз увійти, і він/вона може отримати доступ до різних програм і

послуг. Це полегшує роботу користувача та зводить до мінімуму випадки, коли потрібно запам’ятовувати багато різних паролів.

Керування доступом і авторизація: рішення CIAM керують тим, як і які ресурси дозволено використовувати користувачам на основі ролі та наданих дозволів. Це також допомагає обмежити права користувачів лише на те, що їм потрібно для виконання їхніх робочих функцій, що підвищує безпеку.

Каталогові служби: централізовані служби каталогів відповідають за зберігання та адміністрування ідентифікаційної інформації користувача. Це гарантує, що та сама інформація, що зберігається в усіх програмах і службах, є узгодженою та правильною.

Виявлення загроз і запобігання шахрайству: машинне навчання та аналіз великих даних виявляють загрози та вживають відповідних заходів. Це допомагає в боротьбі з такими діями, як злиття облікових записів і крадіжка особистих даних.

Децентралізована ідентифікація та оркестровка ідентифікації: нові рішення CIAM включають функції DI, що дозволяє користувачам керувати власними ідентифікаційними даними за допомогою блокчейну. Це мінімізує ймовірність великих централізованих втрат даних. Контролює передачу ідентифікаційних даних між різними програмами та системами для підтримки узгодженості політик безпеки, реалізованих на кожному етапі взаємодії клієнта з компанією.

Адаптивна автентифікація: використовує контекст і ризик, щоб змінювати параметри автентифікації залежно від середовища або передбачуваного ризику. Наприклад, він може застосувати MFA для критичних завдань, але дозволити користувачам входити лише за паролями для менш критичних завдань.

CIAM виступає в якості захищеного клієнта, комплексного підходу до захисту даних клієнтів, гарантуючи, що організації можуть надавати безперебійну та безпечну роботу, зберігаючи найвищий рівень довіри користувачів [6].

1. Розширені методи автентифікації: рішення CIAM приділяють велику увагу методам процесу аутентифікації та використання MFA. Це додатково підвищує безпеку, оскільки користувачі будуть змушені надавати інші форми

ідентифікації, окрім своїх паролів, і це неймовірно ускладнює доступ неавторизованих осіб до додатків.

2. Оптимізований єдиний вхід (SSO): CIAM керує логіном SSO, тобто користувач входить лише один раз, щоб отримати доступ до інших програм. Це також покращує взаємодію з користувачем, водночас знижуючи ймовірність інцидентів з паролями, які можуть поставити під загрозу безпеку.

3. Прозора згода користувача: ці системи надають користувачам чіткий спосіб дії щодо того, як буде оброблятися згода, пов’язана з використанням їхніх персональних даних. Користувачі також можуть захистити інформацію, яку вони розкривають, і те, як вона буде використана, створюючи таким чином велику довіру.

4. Надійні механізми контролю доступу: рішення CIAM використовують дуже конкретні політики контролю доступу, які визначають, хто має доступ до даних, і залежно від ролі та привілеїв користувача. Це означає, що лише потрібні люди мають доступ до інформації, що гарантує, що навіть у разі порушення інформації інформація не буде оприлюднена громадськості чи неналежним особам.

5. Захист даних за допомогою шифрування: шифрування даних клієнтів є одним із основних процесів CIAM. Дані в стані спокою, а також дані в русі зашифровані, тому навіть у разі перехоплення дані залишаються в безпеці.

6. Аналітика поведінки та виявлення загроз: платформи CIAM можуть мати розширені функції моніторингу, які шукають порушення в діяльності користувачів. Сповіщення в режимі реального часу може бути згенероване, якщо будь-яка така діяльність відхиляється від звичайної моделі, щоб можна було негайно вжити заходів проти загроз.

Керування ідентифікацією та доступом (IAM) – це структура безпеки та пов’язаний процес, який керує життєвим циклом ідентифікаційних даних користувачів. Це включає керування ідентифікаційними даними від початкової реєстрації до деініціалізації та видалення. IAM регулює, хто може переглядати або отримувати доступ до інформації, керувати даними та виконувати процеси в

кожній системі чи додатку [7].

Основні функції, які підтримує IAM, включають [7]: автентифікація, керування сеансами та маркерами; авторизація; управління політикою; керування профілями користувачів та API CIAM. На рисунку 1.4 наведено приклад типового процесу автентифікації та авторизації для веб-додатка.

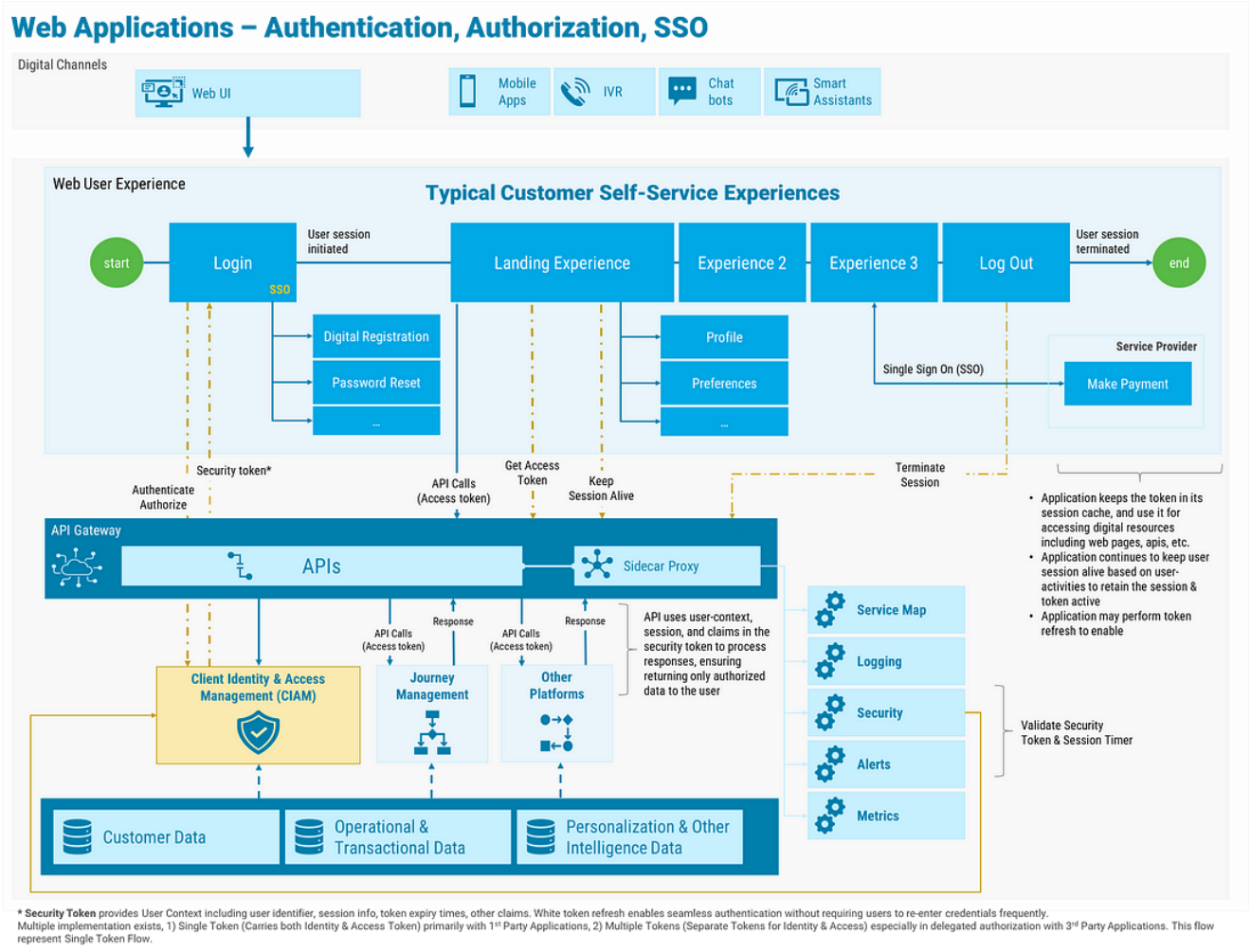

Рис. 1.4. Приклад типового процесу автентифікації
та авторизації для веб-додатка [7]

NIST [8] зазначає, що керування ідентифікацією та доступом (IAM) є основою цифрових послуг. Він являє собою складну оркестровку багатьох технологій, стандартів і протоколів, щоб надати людині доступ до послуг, переваг і даних, на які вона має право. Це також дозволяє організаціям і установам зменшити ризики, пов’язані з шахрайством і несанкціонованим доступом. Таким чином, IAM перебуває на зв’язку між кібербезпекою та клієнтським досвідом, що

робить його ключовим компонентом для створення надійних сучасних цифрових послуг.

Цифрова ідентичність – це унікальне представлення суб'єкта, задіяного в онлайн-транзакції. Цифрова ідентифікація завжди є унікальною в контексті цифрової послуги, але не обов'язково повинна однозначно ідентифікувати суб'єкт у всіх контекстах. Іншими словами, доступ до цифрової послуги може не означати, що особистість суб'єкта в реальному житті відома. Підтвердження особи встановлює, що суб'єкт є тим, за кого себе видає [9].

Цифрова автентифікація – це процес визначення дійсності одного або кількох автентифікаторів, які використовуються для отримання цифрової ідентифікації. Автентифікація встановлює, що суб'єкт, який намагається отримати доступ до цифрової послуги, контролює технології, які використовуються для автентифікації [9].

Успішна автентифікація забезпечує обґрунтовану гарантію, засновану на оцінці ризику, що суб'єкт, який отримує доступ до служби сьогодні, є таким самим, як той, хто раніше отримував доступ до служби. Цифрова ідентифікація є технічною проблемою, оскільки цей процес часто передбачає перевірку автентичності осіб у відкритій мережі та, як правило, передбачає автентифікацію окремих суб'єктів у відкритій мережі для доступу до цифрових державних послуг. Є багато можливостей для видавання себе за іншу особу та інших атак, які шахрайським шляхом заволодіють цифровою ідентичністю іншого суб'єкта [9].

NIST [9] запропонував *Модель цифрової ідентифікації*, яка відображає технології та архітектури, які зараз доступні на ринку. Також доступні більш складні моделі, які розділяють функції такі як видача облікових даних і надання атрибутів, серед більшої кількості сторін, і вони можуть мати переваги в деяких класах програм.

Крім того, певні процеси реєстрації, перевірки ідентифікації та видачі, які виконує CSP, іноді делегуються організації, відомій як орган реєстрації (RA) або менеджер ідентифікації (IM). Типовим є тісний зв'язок між RA і CSP, і природа цього зв'язку може відрізнятися між RA, IM і CSP. Відповідно, термін CSP

включатиме функції RA та IM. Нарешті, CSP може надавати інші послуги на додаток до послуг цифрової ідентифікації.

Цифрова ідентичність – це унікальне представлення суб'єкта, задіяного в онлайн-транзакції. Процес, який використовується для перевірки зв'язку суб'єкта з його реальною ідентичністю, називається перевіркою ідентифікації. У цих настановах сторона, яка підлягає перевірці, називається заявником. Коли заявник успішно завершує процес перевірки, його називають абонентом. Надійність перевірки ідентифікації описується порядковим вимірюванням, яке називається Identity Assurance Level (IAL). На IAL1 перевірка ідентифікації не потрібна, тому будь-яка інформація про атрибути, надана заявником, є самоствердженою або повинна розглядатися як самостверджена та не перевірена (навіть якщо CSP надає RP). IAL2 і IAL3 вимагають перевірки ідентичності, і RP може вимагати від CSP підтвердити інформацію про абонента, таку як перевірені значення атрибутів, перевірені посилання на атрибути або псевдонімні ідентифікатори.

Ця інформація допомагає RP у прийнятті рішень щодо авторизації. RP може вирішити, що йому потрібен IAL2 або IAL3, але йому можуть знадобитися лише певні атрибути, у результаті чого суб'єкт зберігає певний ступінь псевдонімності. Цей підхід до підвищення конфіденційності є перевагою відокремлення надійності процесу перевірки від процесу автентифікації. RP також може використовувати підхід об'єднаної ідентифікації, коли RP передає всю перевірку ідентичності, збір атрибутів і зберігання атрибутів CSP. Сторона, яка підлягає автентифікації, називається заявником, а сторона, яка перевіряє цю особу, називається верифікатором. Коли заявник успішно демонструє верифікатору володіння та контроль над одним або декількома автентифікаторами за допомогою протоколу автентифікації, верифікатор може підтвердити, що заявник є дійсним передплатником. Верифікатор передає твердження про абонента, який може бути псевдонімом або не псевдонімом, до RP. Це твердження містить ідентифікатор і може включати ідентифікаційну інформацію про абонента, таку як ім'я або інші атрибути, які були зібрані в процесі реєстрації (залежно від політики CSP, потреб RP та згоди на розкриття атрибутів, наданої предмет). Якщо

верифікатор також є RP, твердження може бути неявним. RP може використовувати автентифіковану інформацію, надану верифікатором, для прийняття рішень щодо авторизації.

Автентифікація встановлює впевненість у тому, що заявник володіє автентифікатором(ами), прив'язаним до облікових даних, а в деяких випадках і до значень атрибутів підписника (наприклад, якщо абонент є громадянином США, є студентом певного університету або агентством або організацією присвоєно певний номер або код). Автентифікація не визначає повноваження або привілеї доступу заявника; це окреме рішення, яке виходить за рамки цих рекомендацій. RP можуть використовувати автентифіковану особу абонента та атрибути з іншими факторами для прийняття рішень щодо авторизації.

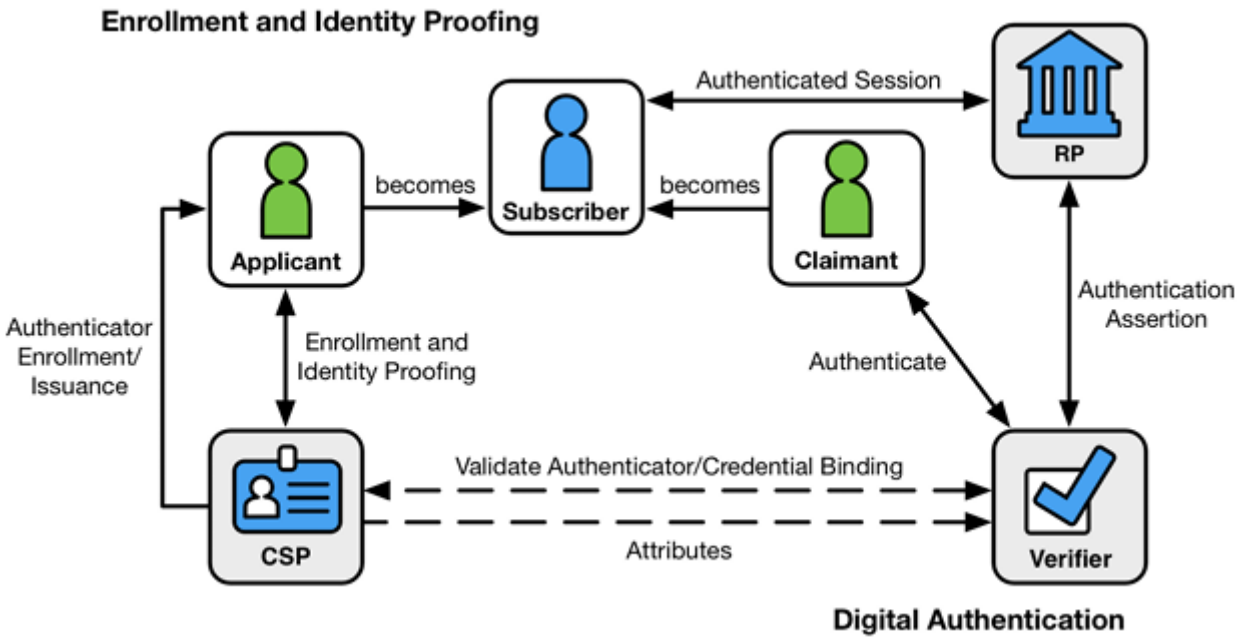

Рис. 1.5. Модель цифрової ідентифікації [9]

Надійність процесу автентифікації описується порядковим вимірюванням, яке називається AAL. AAL1 вимагає однофакторної автентифікації та дозволяється з різними типами автентифікаторів. На AAL2 автентифікація вимагає двох факторів автентифікації для додаткової безпеки. Автентифікація на найвищому рівні, AAL3, додатково вимагає використання апаратного

автентифікатора та стійкості верифікатора до уособлення. Різні сутності та взаємодії, які складають використану модель цифрової ідентифікації, показано на рисунку 1.5.

Ліва частина діаграми показує реєстрацію, видачу облікових даних, дії з керування життєвим циклом і різні стани процесу підтвердження особи та автентифікації. Звичайна послідовність взаємодії така [9]:

1. Заявник подає заявку до CSP через процес реєстрації.

2. CSP підтверджує ідентичність заявника. Після успішної перевірки заявник стає абонентом.

3. Автентифікатор(и) і відповідні облікові дані встановлюються між CSP і абонентом.

4. CSP зберігає облікові дані, їх статус і дані про реєстрацію, зібрані протягом терміну дії облікових даних (як мінімум). Абонент підтримує свій автентифікатор(и).

Інші послідовності менш поширені, але також можуть досягти тих же функціональних вимог.

Права сторона рисунка 1.5 показує об’єкти та взаємодії, пов’язані з використанням автентифікатора для виконання цифрової автентифікації. Абонента називають позивачем, коли йому необхідно пройти автентифікацію в верифікаторі. Взаємодії такі [9]:

1. Заявник доводить верифікатору володіння та контроль над автентифікатором(ами) за допомогою протоколу автентифікації.

2. Верифікатор взаємодіє з CSP, щоб підтвердити облікові дані, які пов’язують особу абонента з його автентифікатором, і, за бажанням, отримати атрибути заявника.

3. CSP або верифікатор надає твердження про абонента до RP, який може використовувати інформацію в твердженнях для прийняття рішення щодо авторизації.

4. Між абонентом і RP встановлюється автентифікований сеанс.

У всіх випадках RP повинен запросити атрибути, які він вимагає, від CSP

перед автентифікацією заявника. Крім того, позивача слід попросити дати згоду на звільнення цих атрибутів перед створенням і звільненням твердження. У деяких випадках верифікатору не потрібно спілкуватися в реальному часі з CSP для завершення автентифікації (наприклад, деякі види використання цифрових сертифікатів). Таким чином, пунктирна лінія між верифікатором і CSP представляє логічний зв'язок між двома об'єктами.

У деяких реалізаціях функції верифікатора, RP і CSP можуть бути розподілені та розділені, як показано на рисунку 1.5. Однак, якщо ці функції знаходяться на одній платформі, взаємодія між компонентами є локальними повідомленнями між програмами, що працюють в одній системі, а не протоколами через спільні ненадійні мережі.

Як зазначалося вище, CSP зберігає інформацію про статус облікових даних, які він видає. Під час видачі облікових даних CSP зазвичай призначають обмежений термін служби, щоб обмежити період обслуговування. Коли статус змінюється або коли термін дії облікових даних закінчується, облікові дані можна оновити або видати повторно; або облікові дані можуть бути анульовані та знищені.

Як правило, абонент проходить автентифікацію в CSP, використовуючи свій існуючий автентифікатор і облікові дані, термін дії яких не закінчився, щоб подати запит на видачу нового автентифікатора та облікових даних. Якщо абонент не надіслав запит на повторну видачу автентифікатора та облікових даних до закінчення терміну їх дії або відкликання, йому може знадобитися повторити процес реєстрації, щоб отримати новий автентифікатор та облікові дані. Крім того, CSP може вирішити прийняти запит протягом пільгового періоду після закінчення.

1.3. Аналіз існуючих рішень для управління ідентифікацією та доступом клієнтів до хмарних сервісів організацій

Рішення Customer Identity and Access Management (CIAM) забезпечують

легкий і безпечний доступ до онлайн-сервісів для клієнтів. Цей тип технології ідентифікації підтримує організації в управлінні ідентифікаційними даними клієнтів, забезпечуючи їм належний доступ із покращеним користувацьким досвідом, без шкоди для безпеки, шляхом застосування безпечної адаптивної багатофакторної автентифікації [11].

Розглянемо рішення CyberArk Customer Identity.

Будучи світовим лідером у сфері безпеки ідентифікаційних даних, CyberArk працює над забезпеченням комплексної безпеки як для ідентифікаційних даних людей, так і для машин, підтримуючи провідні організації в захисті їхніх найважливіших активів. Платформа безпеки CyberArk Identity Security Platform пропонує рішення CAIM у CyberArk Customer Identity, яке розроблено, щоб допомогти динамічним підприємствам наскрізно захищати ідентифікаційні дані клієнтів [11].

Функції ідентифікації клієнта CyberArk:

автентифікація та авторизація доступу за допомогою вбудованого безпечного єдиного входу, контролюючи доступ за допомогою детальних політик;

безпарольна багатофакторна автентифікація на основі штучного інтелекту, з усвідомленням ризиків;

керування ідентифікаторами клієнтів за допомогою API або безпосередньо в Cloud Directory;

повна колекція інструментів розробника, включаючи посібники та інші ресурси, які допомагають розробникам інтегрувати платформу безпеки CyberArk Identity Security;

забезпечення безпеки доступу до бізнес-додатків як для людини, так і для машини;

забезпечення безпеки доступу до ідентифікаційної інформації машини в конвеєрі DevOps;

мінімізація складності і зменшення навантаження на IT-команди.

Підтримувані методи автентифікації: вбудований безпечний єдиний вхід, вхід із соціальної мережі, ім’я користувача та пароль, федеративні облікові дані.

CyberArk Customer Identity дозволяє організаціям безпечно відкривати свої веб-сайти та програми для доступу клієнтів, не залишаючи себе вразливими до порушень безпеки. Користувачі CyberArk Customer Identity високо оцінюють його можливості та надійну підтримку [11].

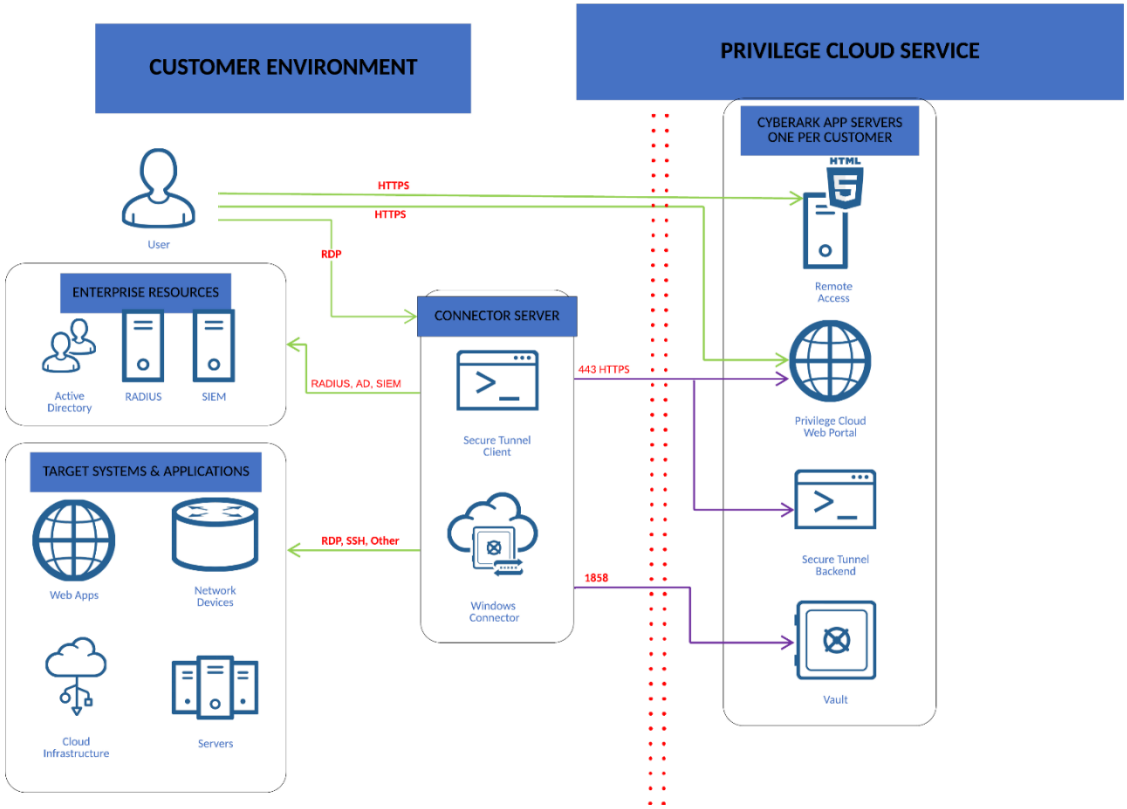

Рис. 1.6. CyberArk Customer Identity [12]

Розглянемо рішення Okta Customer Identity Cloud.

Okta – провідний незалежний постачальник ідентифікаційних даних. Okta надає простий і безпечний доступ до понад 10 000 організацій у всьому світі. Їхня пропозиція CIAM, Okta Customer Identity Cloud, підтримує організації у вирішенні складних проблем ідентичності, дозволяючи їм впроваджувати інновації та масштабувати без проблем [11].

Функції Okta Customer Identity Cloud [11]:

надає інтелектуальний доступ через адаптивну багатофакторну автентифікацію (MFA), яка вивчає поведінку клієнтів під час входу та адаптується

відповідно;

за допомогою системи єдиного входу (SSO) користувачам потрібно ввійти лише один раз і отримати доступ до всіх пов'язаних програм через автентифікацію імен користувачів і паролів, вхід через соціальні мережі або корпоративну федерацію;

забезпечує автентифікацію користувачів у всіх додатках за допомогою універсального входу;

забезпечує корпоративну федерацію, використовуючи готові інтеграції з поширеними корпоративними системами ідентифікації;

забезпечує візуальне «перетягування» для налаштування потоку ідентичності відповідно до корпоративних вимог:

забезпечує захист від різноманітних атак за допомогою виявлення зламаного пароля, виявлення ботів і обмеження підозрілих IP-адрес;%

створює індивідуальні робочі процеси автентифікації та авторизації для клієнтів B2B у масштабі.

Підтримувані методи автентифікації: єдиний вхід, багатофакторна автентифікація, робочі процеси автентифікації та авторизації, біометрія, ключі безпеки, токени M2M.

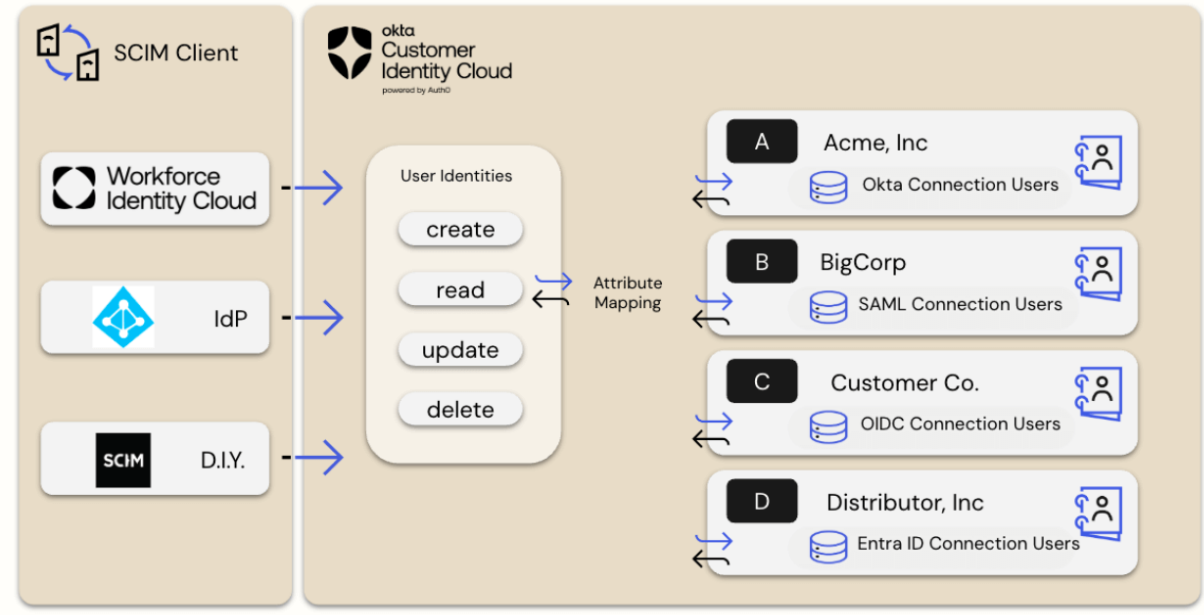

Рис. 1.7. Okta Customer Identity Cloud [13]

В [11] відмічається, що користувачі хвалять рішення Okta Customer Identity за її функціональність, бездоганний підхід і простоту використання. Понад 16 400 організацій покладаються на Okta, щоб допомогти їм забезпечити своїх клієнтів і робочу силу. Фахівці [11] рекомендують це рішення будь-яким організаціям, які хочуть захистити споживчі програми та програми SaaS, зберігаючи при цьому оптимізований цифровий досвід.

Azure AD B2C – це рішення для керування доступом до особистих даних клієнтів (CIAM), здатне підтримувати мільйони користувачів і мільярди автентифікацій на день. Він керує масштабуванням і безпекою платформи автентифікації, контролює її та автоматично обробляє такі загрози, як відмова в обслуговуванні, підбір пароля або атаки грубою силою [14].

Azure AD B2C є окремою службою від Azure Active Directory (Azure AD). Він побудований на тій самій технології, що й Azure AD, але з іншою метою. Це дозволяє компаніям створювати клієнтські програми, а потім дозволяє будь-кому реєструватися в цих програмах без обмежень щодо облікових записів користувачів [14].

Деякі з основних переваг використання Azure AD B2C [14]:

інтеграція з обліковими записами соціальних мереж, такими як Facebook або Google+, вимагає додаткової роботи. Завдяки використанню Azure AD B2C ця робота перекладається на Microsoft, і розробники можуть більше зосередитися на основних функціях, які потрібно розробити в додатку. Azure AD B2C також підтримує багатофакторну автентифікацію та самостійне скидання пароля, застосовуючи деякі базові конфігурації;

впровадження Azure AD B2C є дуже економічно ефективним завдяки розумній ціні порівняно з іншими постачальниками або розробці власної системи керування ідентифікацією. Перші 50 000 автентифікацій і користувачів безкоштовні;

система автентифікації, яку надає Azure AD B2C, дуже безпечна для захисту ідентифікаційних даних користувача та облікових даних. Azure AD B2C надає ідентифікацію як послугу для корпоративних додатків, підтримуючи два

галузевих стандартних протоколи OpenID Connect і OAuth 2.0.

Будь-яка компанія або окрема особа, яка бажає автентифікувати кінцевих користувачів у своїх веб-/мобільних додатках за допомогою рішення автентифікації білої мітки. Окрім автентифікації, служба Azure AD B2C використовується для авторизації, наприклад доступу до ресурсів API автентифікованими користувачами. Azure AD B2C призначено для використання IT-адміністраторами та розробниками. На рисунку 1.8. показано потік даних для входу в Azure AD B2C.

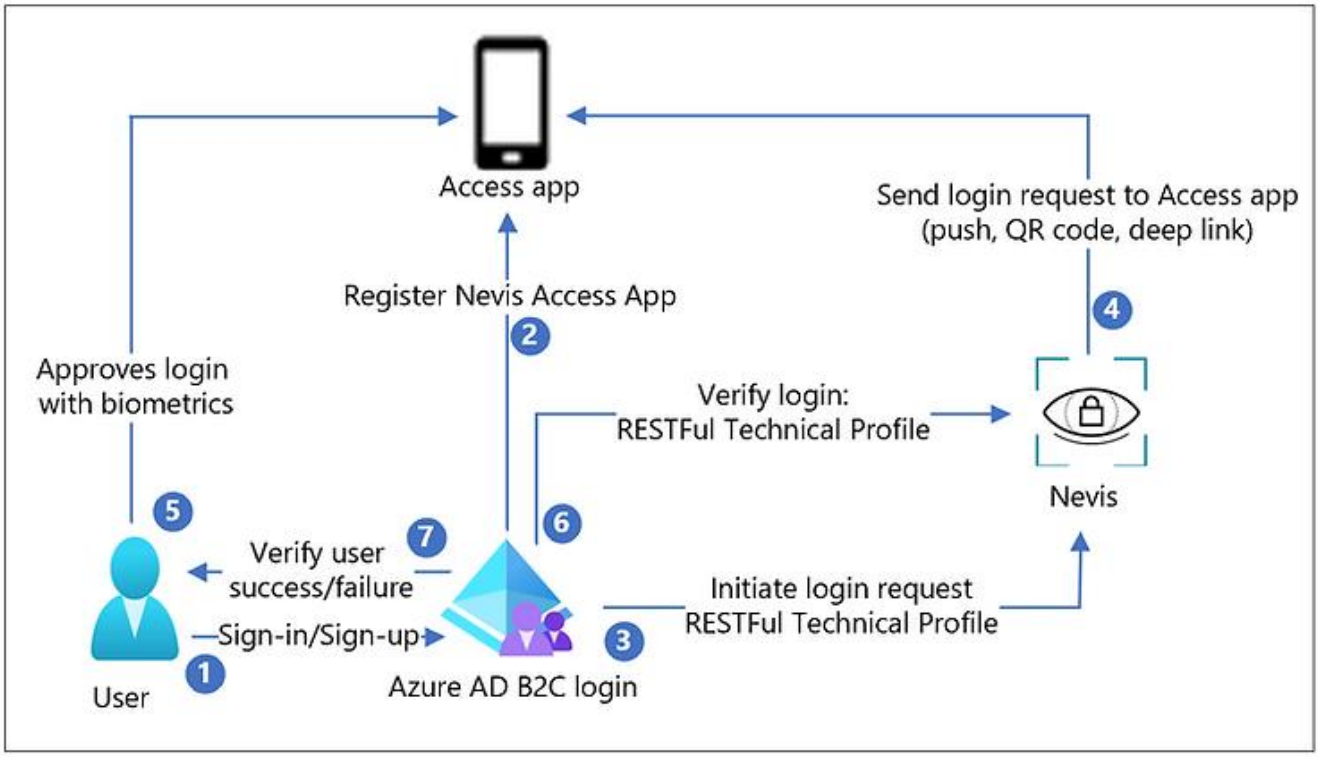

Рис. 1.8. Потік даних для входу в Azure AD B2C [14]

Отже, у сучасному цифровому світі безперебійний досвід клієнтів стає необхідністю. Клієнти очікують, що вони зможуть без зусиль зареєструватися, увійти в систему та отримати доступ до необхідних послуг на різних платформах. Ось де на допомогу приходить Customer Identity and Access Management (CIAM).

CIAM стало цифровою основою, яка забезпечує безпечну та зручну взаємодію з клієнтами. Це набір технологій і процесів, які керують тим, як клієнти ідентифікують себе та отримують доступ до онлайн-ресурсів організації.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ТА ДОСТУПОМ КЛІЄНТІВ ДО ХМАРНИХ СЕРВІСІВ ОРГАНІЗАЦІЇ НА БАЗІ AKAMAI IDENTITY CLOUD

2.1. Призначення та основні функції рішення Akamai Identity Cloud

Споживачі цифрових технологій очікують безперебійної взаємодії з брендом онлайн, яка є персоналізованою, безпечною та конфіденційною. Рішення Akamai для ідентифікації клієнтів і керування доступом (CIAM) Identity Cloud забезпечує швидке розгортання єдиного входу (SSO), реєстрації та автентифікації.

Рішення Akamai Identity Cloud дає змогу керувати згодою та налаштуваннями відповідно до нормативних вимог на гнучкій платформі, яка масштабується за варіантами використання, регіонами, правилами та підтримує мільйони користувачів. Вибір багатьох найбільших брендів у всьому світі, Identity Cloud забезпечує широкомасштабну адаптацію споживачів, настроювані робочі процеси для підтримки найширшого досвіду додатків і високопродуктивну хмарну інфраструктуру для інтелектуального пристосування до стрибків використання. Завдяки повному набору панелей маркетингу та IT аналітики та інтеграції з усіма основними рішеннями MarTech, Identity Cloud є вибором CIAM серед споживчих брендів великого обсягу [5].

Створене на платформі Akamai Intelligent Edge Platform, Identity Cloud забезпечує безпечний і масштабований CIAM для великих брендів, які орієнтуються на споживачів. Identity Cloud пропонує впровадження на основі API та SDK для підтримки широкого спектру повністю налаштованих випадків використання, які швидко виходять на ринок.

Ідентифікаційна хмара як хмарне програмне забезпечення як послуга (SaaS) розроблена для інтелектуального масштабування, щоб гарантувати, що реєстрація клієнтів, автентифікація та функції SSO завжди доступні та працюють із найменшою затримкою. Гнучкі схеми даних і робочі процеси можуть

підтримувати майже будь-який варіант використання, орієнтований на споживача. З самого початку платформа ідентифікації Akamai була розроблена, щоб надати глобальним брендам та їхнім клієнтам необхідне управління даними та доступність. Простіше кажучи, Identity Cloud забезпечує безперебійну, безпечну та масштабовану роботу клієнтів [5].

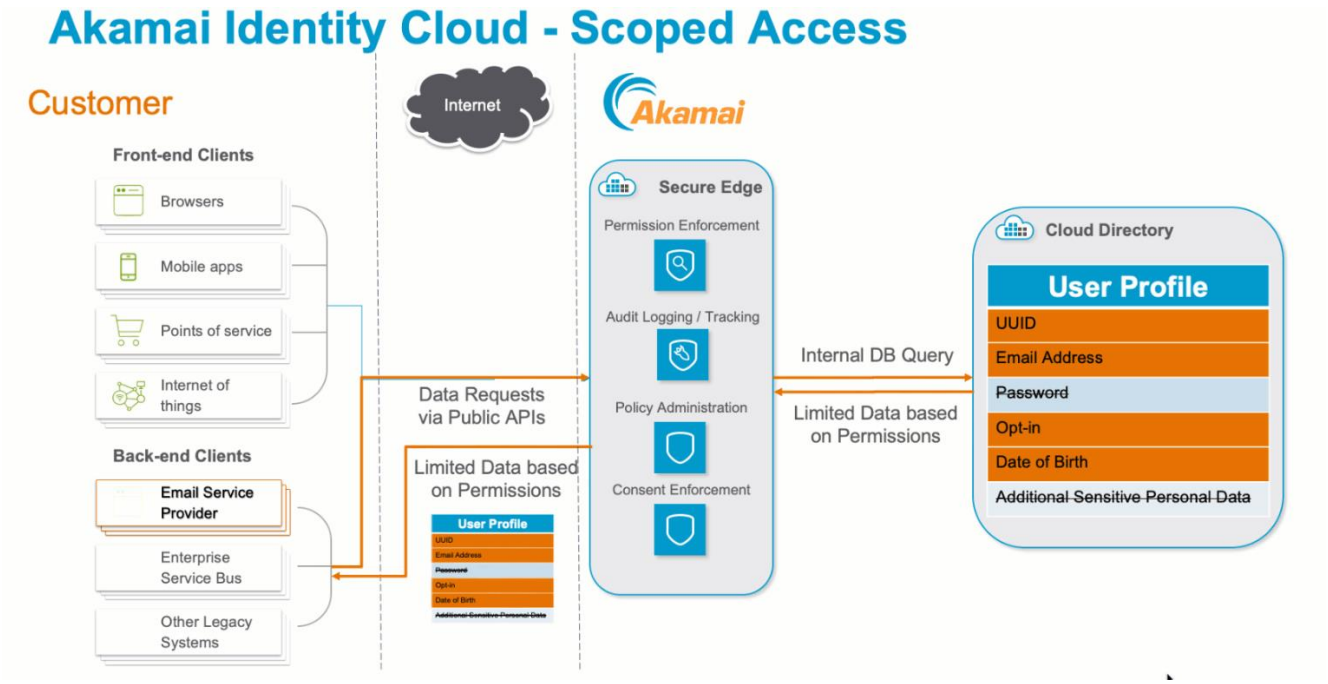

Рис. 2.1. Компоненти рішення Akamai Identity Cloud

Централізація управління ідентифікацією споживача

Identity Cloud легко інтегрується у корпоративну інфраструктуру ідентифікації, надаючи організації центральне та гнучке рішення для керування великою кількістю ідентифікаційних даних клієнтів. Гнучкі схеми Identity Cloud можуть задовольнити потреби корпоративних розробників і маркетингових команд. Identity Cloud може діяти як центральне керування основними даними (MDM) для конкретної організації або легко інтегруватися з уже існуючими системами керування даними, продажами та автоматизацією маркетингу.

Забезпечення надійного, сумісного споживчого досвіду

Реєстрація клієнта повинна бути можливою в будь-який час. Identity Cloud пропонує неперевершений час безперебійної роботи, а його глобальний відбиток

даних і інтелектуальне масштабування розроблені для того, щоб гарантувати, що раптове збільшення трафіку не призведе до зниження продуктивності. Гнучкі схеми даних дозволяють ділитися даними корпоративних клієнтів з іншими системами та платформами автоматизації маркетингу відповідно до правил захисту даних.

Дотримання вимог щодо конфіденційності даних споживача

Збирати дані споживачів легко, але зробити це в нову епоху глобальних правил конфіденційності значно складніше. Загальний регламент ЄС із захисту даних (GDPR), Каліфорнійський закон про конфіденційність споживачів (CCPA), канадський Закон про захист особистої інформації та електронних документів (PIPEDA) та інші регіональні нормативні акти щодо споживчих даних покладають на бренди обов'язок відстежувати та розуміти дані, які вони збирають. і надавати параметри керування конфіденційністю безпосередньо споживачам. Identity Cloud дозволяє поступово створювати профілі та керувати згодою та вподобаннями клієнтів, перетворюючи ці нові правила на можливості побудувати довірчі стосунки з корпоративними клієнтами, що в кінцевому підсумку призведе до підвищення лояльності до бренду та кращого бізнесу.

Ключові можливості рішення Akamai Identity Cloud [5]:

Безпроблемна та безпечна автентифікація та SSO: Identity Cloud надає найширший набір методів автентифікації, включаючи вхід у соціальні мережі, служби каталогів і OpenID Connect (OIDC), а також контроль доступу на основі ролей і атрибутів (RBAC і ABAC), а також контроль доступу на основі ризиків і кількох Параметри автентифікації з фактором – для безпечного доступу та SSO у вашій екосистемі.

Гнучкі розгортання: методи розгортання на основі API підтримують широкий спектр налаштувань і варіантів використання, тоді як розгортання на основі SDK дозволяють швидко вивести на ринок кілька програм. Гнучкі схеми даних були розроблені з самого початку для підтримки найширшого спектру випадків використання, спрямованих на клієнтів.

Масштабованість і доступність: Identity Cloud спеціально розроблено для

задоволення потреб великого обсягу керування ідентифікацією клієнтів. Від регіональної диференціації до керування стрибками споживчого використання, хмарне рішення CIAM від Akamai пропонує нашим клієнтам неперевершену масштабованість і доступність.

Аналіз та інтеграції: вбудовані інформаційні панелі Identity Cloud дають маркетинговим та IT-командам змогу в режимі реального часу бачити дані про дії клієнтів, допомагаючи зрозуміти фактори, що впливають на шлях клієнта, і різницю між законною та шахрайською реєстраціями.

Варіанти конфіденційності клієнтів, що відповідають нормам: Identity Cloud пропонує швидкі рішення для підтримки дотримання GDPR, CCPA, PIPEDA та інших регіональних нормативних актів щодо споживчих даних, включаючи керування вподобаннями клієнтів, обмежений доступ до споживчих даних і централізоване керування споживанням даних нижчими системами.

Переваги для бізнесу, які надає рішення Akamai Identity Cloud [5]:

покращує адаптацію клієнтів за допомогою швидкої реєстрації та автентифікації, включаючи SSO та параметри входу через соціальні мережі, а також повну статистику дій відвідувачів під час входу;

забезпечує масштабування для багатьох користувачів і випадків використання за допомогою хмарної глобальної архітектури, створеної за допомогою схеми даних і хмари можливості зберігання для обробки складних випадків використання та мільйонів користувачів;

забезпечує відповідність і безпеку даних за допомогою засобів контролю даних, спрямованих на споживача, і захисту даних на платформі Akamai Intelligent Edge Platform;

розширює видимість клієнтів в організації за допомогою реєстрації та автентифікації в реальному часі, моніторингу даних про діяльність і можливості сегментувати дані про діяльність за регіонами та спеціальними сегментами;

забезпечує налаштований користувальницький досвід за допомогою впровадження першочергового API та гнучких схем даних, призначених для складної інтеграції та персоналізованого досвіду користувача;

зводить до мінімуму ризики безпеки ідентифікаційної інформації клієнта, використовуючи розгортання на основі SDK для розміщення реєстрації, автентифікації та керування даними клієнтів у рамках захисту Akamai Intelligent Edge Platform.

2.2. Архітектура рішення Akamai Identity Cloud

Рішення CIAM зазвичай надаються як хмарні служби, які розміщуються та керуються надійною третьою стороною для максимальної простоти, гнучкості та масштабованості. Необхідно підкреслити, що збираючи та обробляючи дані клієнтів, організації повинні дотримуватися багатьох правил захисту даних і конфіденційності. Рішення для керування ідентифікацією, наприклад Akamai Identity Cloud, може допомогти впоратися з цими проблемами.

Розглянемо зміст технології управління ідентифікацією та доступом клієнтів за допомогою Akamai Identity Cloud (рисунок 2.2) [3]:

1. Кінцевий користувач отримує доступ до цифрових ресурсів компанії з різних каналів (браузерів для настільних комп’ютерів, мобільних додатків, Інтернету речей) часто використовуючи вхід із соціальної мережі.

2. Граничні сервери захищають загальнодоступні веб-додатки, сторінки входу та сторінки реєстрації від DDoS-атак і атак веб-додатків.

3. Керування ботом виявляє та пом’якшує автоматичні загрози, зокрема сканування веб-сторінок і надсилання облікових даних.

4. Платформа Akamai Intelligent Edge і її рішення безпеки захищають Akamai Identity Cloud від зловмисних атак.

5. Akamai Intelligent Edge Platform направляє законний трафік на сторінки реєстрації та входу в цифрові ресурси компанії.

6. Akamai Identity Cloud допомагає підприємствам дотримуватися відповідних норм захисту даних.

7. Akamai Identity Cloud – це рішення ідентифікації як послуги (Identity as a Service, IDaaS), яке дозволяє організаціям надавати кінцевим користувачам

контроль над створенням, використанням і керуванням їхніми даними.

8. Центральна база даних профілів клієнтів є єдиним джерелом правдивих відомостей про ідентифікацію кінцевих користувачів і права доступу.

9. Клієнти можуть отримувати доступ, переглядати, редагувати та відкликати згоду за допомогою централізованого самообслуговування.

10. Контроль доступу до рівня окремих полів запису даних як для користувачів, так і для додатків.

11. Akamai Identity Cloud інтегрується зі сторонніми системами для подальшої обробки даних клієнтів, наприклад стека маркетингових технологій.

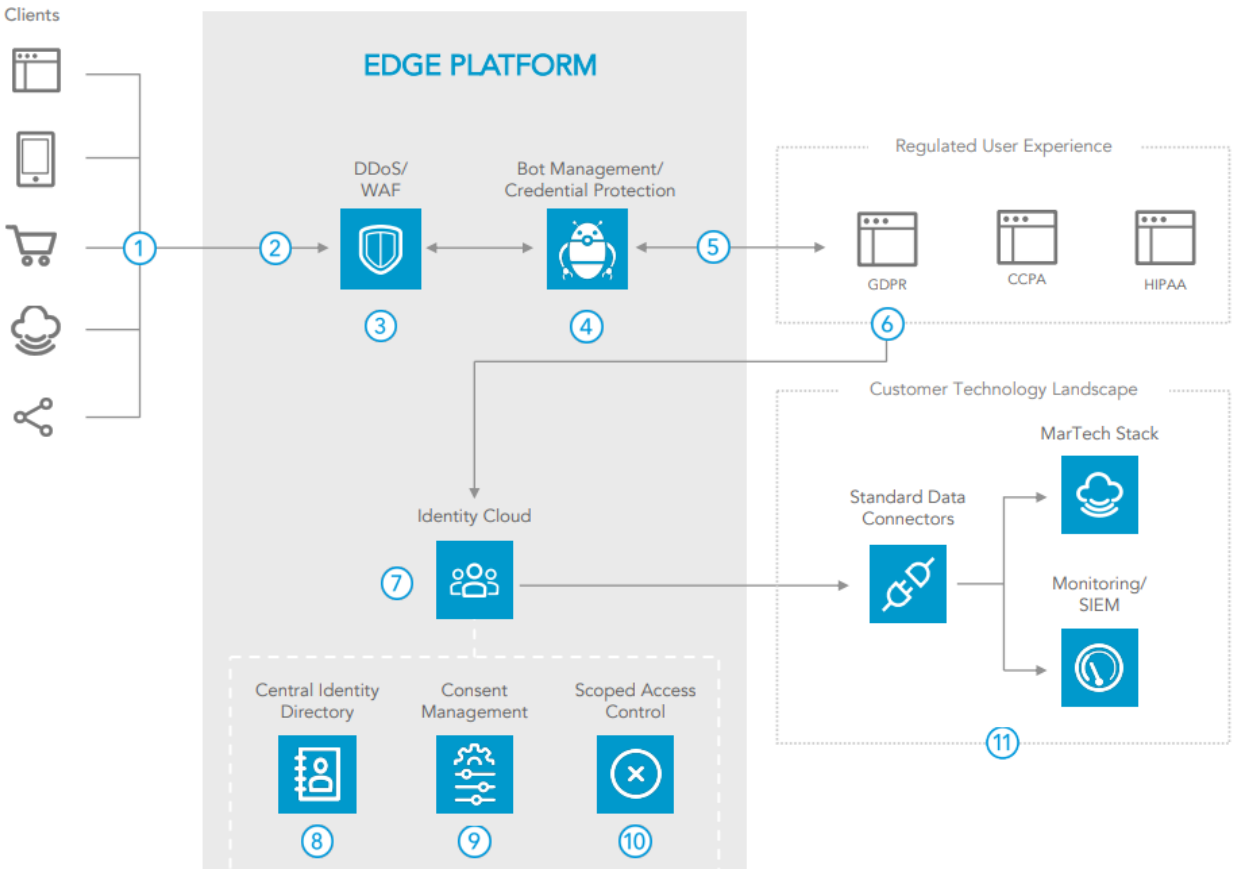

Рис. 2.2. Схема реалізації технології управління ідентифікацією та доступом клієнтів за допомогою Akamai Identity Cloud [3]

Як продукт керування інформацією та доступом клієнтів (CIAM), основна задача Akamai Identity Cloud полягає в тому, щоб дозволити користувачам створювати облікові записи у корпоративному додатку чи на веб-сайті, а потім

мати можливість повернутися на цей веб-сайт чи додаток та увійти до свого облікового запису [4].

Щоб допомогти керувати логінами та реєстраціями, функція розміщеного входу Akamai Identity Cloud широко використовує як OAuth, так і OpenID Connect, пропонуючи підтримку для таких речей, як різні типи дозволів, різні типи відповідей і режимів, а також широкий спектр областей і претензій (включаючи спеціальні претензії) [4].

Отже, рішення Akamai Identity Cloud забезпечує клієнтам винятковий досвід користувача під час створення, використання та керування особистими обліковими записами. Akamai Identity Cloud дозволяє реалізувати високу масштабованість на основі програмного забезпечення як послуги (SaaS), яке може обробляти сотні мільйонів ідентифікацій. Akamai Identity Cloud реалізує функції сервера для керування обліковими записами та контролювати їх, а також зберігати, аналізувати та звітувати про дані профілів клієнтів. Це рішення працює на всіх додатках і підключених пристроях, щоб уніфікувати та захистити ідентифікаційні дані відповідно до нормативних вимог.

2.3. Керування входом і реєстрацією користувачів в Akamai Identity Cloud

Керування двофакторною автентифікацією (2FA)

Ми можемо додати другий рівень безпеки для входу та реєстрації користувачів. За допомогою двофакторної автентифікації користувач входить у систему й одразу отримує код доступу електронною поштою чи текстовим повідомленням. Користувач повинен ввести цей код доступу, перш ніж отримати доступ, ідентифікаційні номери та маркери оновлення.

Двофакторна автентифікація (2FA) допомагає посилити захист, додаючи другий фактор автентифікації: окрім адреси електронної пошти та пароля вам потрібна друга інформація, перш ніж ви зможете увійти та отримати доступ до облікового запису. У випадку Hosted Login v2 цією додатковою інформацією є

одноразовий код доступу (тобто одноразовий пароль), надісланий користувачеві електронною поштою або текстовим повідомленням (за допомогою SMS: служба коротких повідомлень). Перед тим, як користувач повністю ввійде в систему, і перед тим, як йому буде видано маркер доступу, цей користувач повинен надати надісланий йому код доступу. Якщо немає коду доступу, тоді ви не зможете увійти в систему та не зможете отримати маркер доступу.

Коди доступу – це випадково згенеровані шестизначні значення, прив'язані до конкретного облікового запису користувача. Наприклад, якщо користувачу *karim.nafir@mail.com* надіслано код 036858, то лише *karim.nafir@mail.com* може використовувати цей код. Якщо будь-який інший користувач представить код підтвердження, він буде відхилений як недійсний (рисунок 2.3).

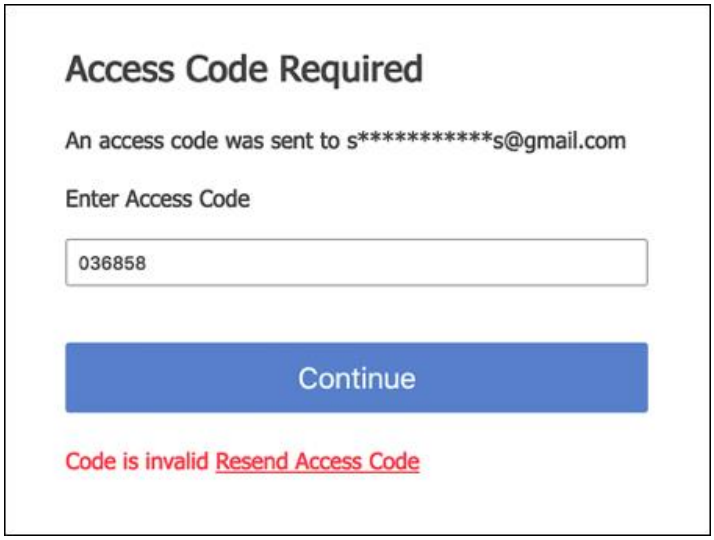

Рис. 2.3. Відхилення спроби доступу

Термін дії кодів доступу закінчується через 10 хвилин; якщо користувач чекає 11 хвилин, щоб ввести код, цей код буде відхилено, і користувачеві потрібно буде подати запит на новий.

Коди можна використовувати лише один раз, хоча користувач може мати більше одного дійсного коду доступу. Наприклад, припустімо, що користувач увійшов у систему, і в рамках процесу 2FA йому було надіслано код доступу. Однак замість використання цього коду користувач запитує інший код. Цей

другий код також надсилається; однак перший код не буде відкликано чи іншим чином визнано недійсним. Це означає, що тепер у користувача є два дійсних коди підтвердження, і кожен з них можна використовувати для завершення процесу 2FA. Це одна з причин, чому коди підтвердження мають такий обмежений термін служби: щоб мінімізувати наслідки для безпеки, якщо користувач має кілька дійсних кодів 2FA. Хоча, оскільки коди прив’язані до певного облікового запису, ці ризики для безпеки відносно незначні.

У Hosted Login v1 ми можемо створити новий обліковий запис одним із двох способів:

вказавши адресу електронної пошти та пароль. Це відоме як «традиційна» реєстрація;

увійшовши до постачальника соціальних даних, наприклад Facebook або Twitter, і використовуючи наявний обліковий запис цього постачальника як свій обліковий запис Identity Cloud. Після того, як ви увійшли до свого соціального провайдера, вам потрібно буде вказати адресу електронної пошти (а також будь-які інші необхідні атрибути), перш ніж ваш обліковий запис буде створено.

Незалежно від способу створення облікового запису, ми ввійдемо в систему одразу після створення облікового запису. Крім того, нам буде надіслано електронний лист для підтвердження електронної адреси (рисунок 2.4).

Тепер давайте порівняємо це з процесом реєстрації користувача в Hosted Login v2 (або, точніше, з процесом реєстрації з увімкненим 2FA). Як і Hosted Login v1, ми можемо створити новий обліковий запис за допомогою традиційної реєстрації або соціальної реєстрації. Однак у цьому випадку ми не входимо в систему одразу після натискання кнопки для створення нового облікового запису. Натомість на адресу електронної пошти, яку ми вказали під час реєстрації, буде надіслано код доступу (випадкове шестизначне число). Крім того, з’явиться екран «Потрібен код доступу» (рисунок 2.5).

Ми маємо отримати код підтвердження, надісланий електронною поштою, ввести цей код у поле «Введіть код доступу», а потім натиснути «Продовжити». Тільки тоді ми увійдемо в систему, і тільки тоді нам буде видано маркер доступу.

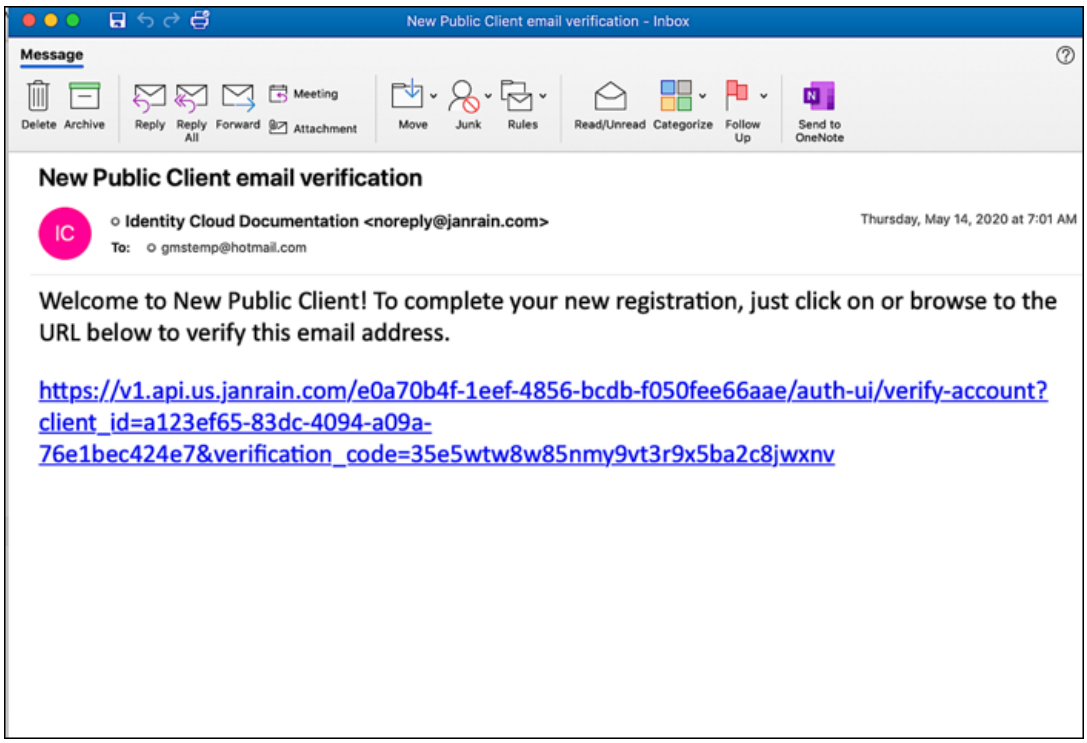

Рис. 2.4. Лист для підтвердження електронної адреси

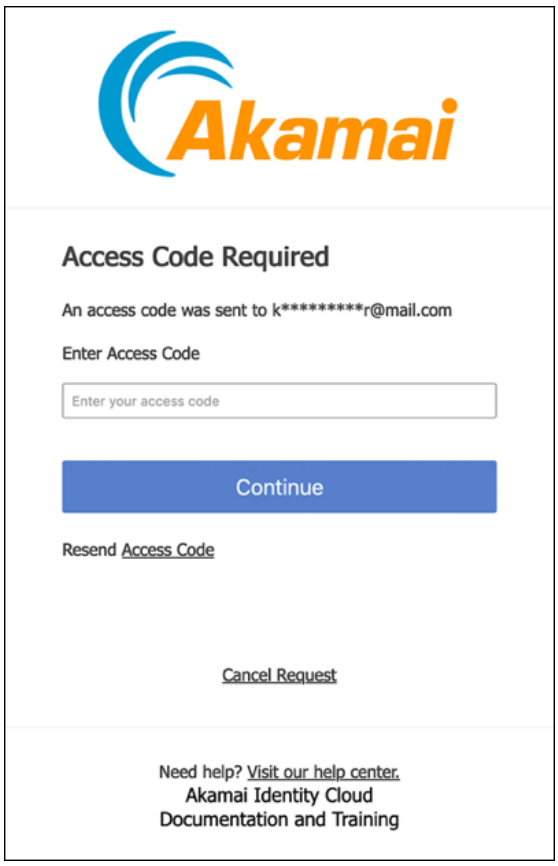

Рис. 2.5. Запит код доступу

Тут слід пам’ятати дві речі. У нас є 10 хвилин, щоб надати код доступу. Це тому, що термін дії кодів закінчується через 10 хвилин. Якщо ми чекаємо надто довго або якщо введемо недійсний код, реєстрація буде призупинена. Якщо це станеться, просто натисніть *Повторно надіслати код доступу* та подати запит на новий код.

До речі, термін дії коду доступу за умовчанням (10 хвилин) не можна налаштувати.

Під час реєстрації коди доступу надсилаються лише на електронну пошту. Однак після створення облікового запису ми зможемо отримати коди, надіслані електронною поштою або текстовим повідомленням.

2FA та логіни користувачів

Якщо ввімкнено двофакторна автентифікація вона також починає діяти щоразу, коли користувач входить на корпоративний веб-сайт або в додаток. Коли користувач відвідує сайт, йому відкривається стандартний екран входу. Потім вони входять, ввівши адресу електронної пошти та пароль (традиційний вхід), або натиснувши кнопку постачальника соціального входу та ввійшовши до постачальника соціальних даних (соціальний вхід). Якщо це схоже на те, як користувачі входять у систему, коли 2FA не ввімкнено, що ж, на це є вагома причина: користувачі спочатку входять однаково, незалежно від того, чи використовується 2FA.

Різниця виникає після того, як користувач увійшов у систему та пройшов автентифікацію. Після входу користувача, але до того, як йому або їй буде видано маркер доступу, Hosted Login перевіряє профіль користувача, щоб дізнатися, чи містить цей профіль адресу електронної пошти та номер мобільного пристрою. (Чому ці два пункти? Тому що це два способи, якими виконується 2FA: або електронною поштою з кодом доступу користувачеві, або текстовим повідомленням з кодом доступу на мобільний пристрій користувача.) Якщо користувач надав адресу електронної пошти та номер мобільного пристрою, з’явиться екран «Потрібен 2FA» (рисунок 2.6).

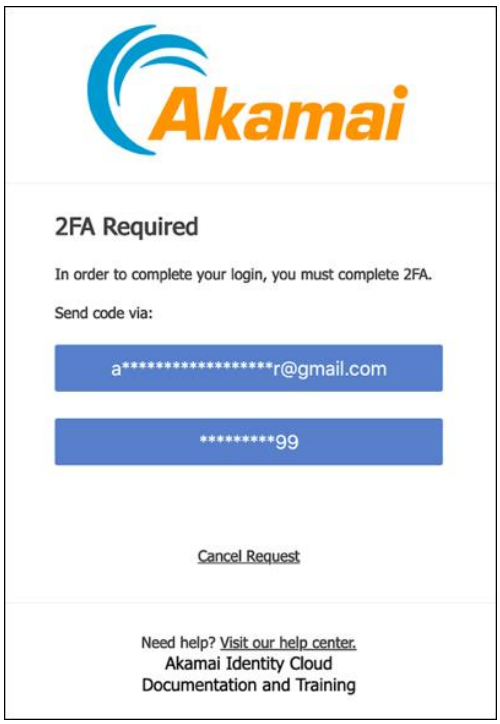

Рис. 2.6. Запит фактора 2FA

Якщо користувач вказав лише адресу електронної пошти, код підтвердження автоматично надсилається на адресу електронної пошти користувача, а екран із вимогою 2FA не відображається.

На екрані «Потрібна 2FA» (якщо користувач має адресу електронної пошти та номер мобільного пристрою) він натискає потрібний метод 2FA (електронна пошта або текстове повідомлення), і код підтвердження буде надіслано. Одночасно з’явиться екран «Потрібен код доступу». Користувач повинен ввести дійсний код і натиснути «Продовжити», перш ніж йому буде видано маркер доступу.

Автентифікація на основі ризиків

Коли мова заходить про керування цифровими ідентифікаторами, безпека має першочергове значення: жодна організація не хоче збирати особисту інформацію користувачів лише для того, щоб ця інформація потрапила в руки хакерів і зломщиків. Якщо ви коли-небудь замислювалися, чому вам потрібно вводити ім’я користувача та пароль, вказувати дівоче прізвище вашої матері та відповідати на текстове повідомлення, надіслане на ваш мобільний телефон, і вибирати всі зображення, на яких зображено велосипед, тепер ви знаєте: це все це

частина зусиль, щоб захистити вашу цифрову ідентичність.

Для продуктів Customer Identity and Access Management, таких як Akamai Identity Cloud, хитрість полягає в тому, щоб спробувати збалансувати безпеку та плавну та ненав’язливу взаємодію з користувачем. Наприклад, припустімо, що у вас є сайт електронної комерції. У такому випадку ви можете:

для перегляду елементів, доступних на сайті, не потрібна автентифікація;

вимагати простого входу (наприклад, імені користувача та пароля), щоб дозволити користувачам додавати вибрані товари до своїх кошиків для покупок. Щоб спростити процес, ці логіни можна навіть зробити «закріпленими». Тобто після автентифікації користувача його сеанс входу може бути встановлений на тривалий період часу (скажімо, 30 днів). Якщо користувач не вийде з системи або іншим чином не завершить цей сеанс, користувач може повернутися на сайт у будь-який час протягом наступних 30 днів і додати товари до свого кошика для покупок без повторного входу;

вимагати додатковий фактор автентифікації (наприклад, введення коду, надісланого за допомогою текстового повідомлення), лише коли користувач готовий вийти з покупки та надіслати своє замовлення.

Це означає:

діяльність із низьким рівнем ризику (наприклад, перегляд сайту) не вимагає автентифікації;

діяльність із помірним ризиком (наприклад, додавання товарів у кошик для покупок) вимагає помірної автентифікації;

діяльність із вищим ризиком (наприклад, використання облікового запису для купівлі товарів) вимагає пропорційно вищого рівня автентифікації.

Цей підхід часто називають «автентифікацією на основі ризику» (Risk-based authentication, RBA), методологією, за якої необхідна автентифікація буде змінюватися залежно від ризику пов’язаної діяльності.

Впроваджуючи дві нові претензії – претензії *acr* і *amr* – для розміщеного входу, Identity Cloud спрощує для додатків розробку шляхів клієнта, які збалансовують безпеку та взаємодію з користувачем.

Як працює автентифікація на основі ризиків?

RBA дозволяє визначити рівень автентифікації, необхідний для виконання певної діяльності. Наприклад, припустімо, що для того, щоб отримати доступ до свого кошика для покупок і відправити замовлення, нам потрібно авторизуватися за допомогою адреси електронної пошти та пароля, а також нам потрібно пройти двофакторну авторизацію.

Претензія acr у маркері ідентифікації

Акронім *acr* є скороченням від Authentication Context Class Reference, і в цьому випадку стосується заяви *acr*, яка додається до маркера ідентифікації; наприклад, якщо ми використовуємо RBA, то наш маркер ідентифікації може містити претензію, яка виглядає так: *"acr": 2.*

Це твердження можна вважати нашою «оцінкою» автентифікації, і, як і багато інших оцінок, чим вище, тим краще. Значення, присвоєні претензії *acr*, базуються на методології, викладеній у Рекомендаціях щодо цифрової ідентифікації NIST (спеціальна публікація NIST 800-63-3).

Як правило, користувачі починають з оцінки *acr 0*.

Якщо користувач автентифікується за допомогою адреси електронної пошти та пароля, значення *acr* збільшується на 1. Це означає, що якщо користувач успішно автентифікований шляхом введення адреси електронної пошти та пароля, користувач матиме *acr 1*: початкове значення 0 плюс 1, доданий до його рахунку після успішного входу.

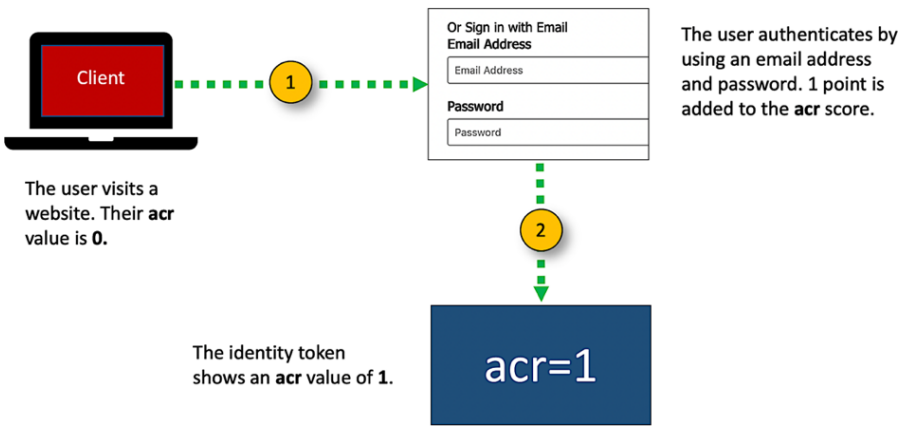

Рис. 2.7. Отримання *acr 1*

Якщо користувач використовує SMS або електронну пошту для завершення двофакторної автентифікації, значення *acr* збільшується на 1. Наприклад, припустімо, що користувач увійшов на веб-сайт, використовуючи адресу електронної пошти та пароль, а потім завершив двофакторну автентифікацію, вказавши код доступу, надісланий через SMS-повідомлення. Цей користувач матиме значення *acr 2*: початкове значення 0 плюс 1 після входу за допомогою своєї адреси електронної пошти та пароля плюс ще 1 після завершення двофакторної автентифікації через SMS. Іншими словами, користувач використовував два різні методи автентифікації (адреса електронної пошти/пароль і двофакторна автентифікація через SMS). Отже, вони отримують значення *acr 2*.

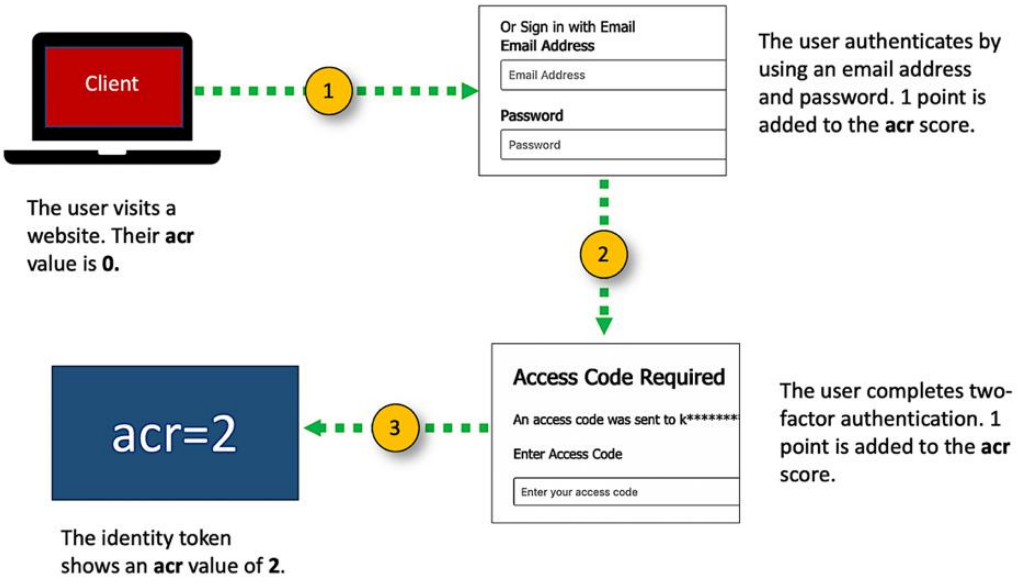

Рис. 2.8. Отримання *acr 2*

Зверніть увагу, що користувач також може отримати значення *acr 2*, увійшовши в систему за допомогою електронної адреси та пароля, а потім пройшовши двофакторну автентифікацію, ввівши код доступу, надісланий на його обліковий запис електронної пошти. Це в сумі становить значення *acr 2*: початкове значення 0 плюс 1 після входу в систему за допомогою адреси електронної пошти та пароля плюс 1 після завершення двофакторної автентифікації.

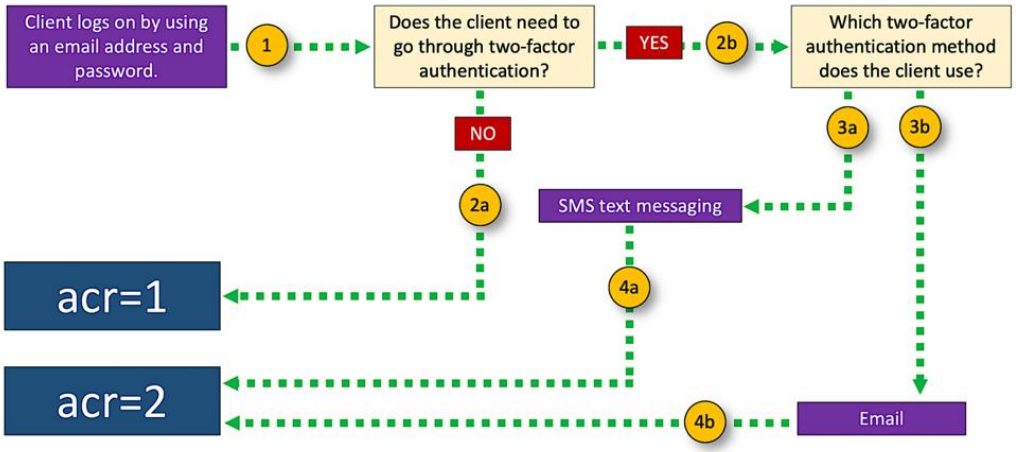

Рис. 2.9. Різні способи отримання *arc*

І так, так чи інакше, ми отримуємо оцінку *acr 2*. Важливим є сам результат, а не обов'язковий шлях, який ви пройшли, щоб досягти цього результату.

Користувачам потрібен лише мінімальний дозвіл для виконання деяких дій (наприклад, перегляду корпоративного сайту). Для інших дій їм може знадобитися надати додатковий рівень автентифікації.

Індивідуальні рівні претензій *acr*, які використовує Hosted Login, базуються на рівнях гарантії автентифікатора (AAL) NIST.

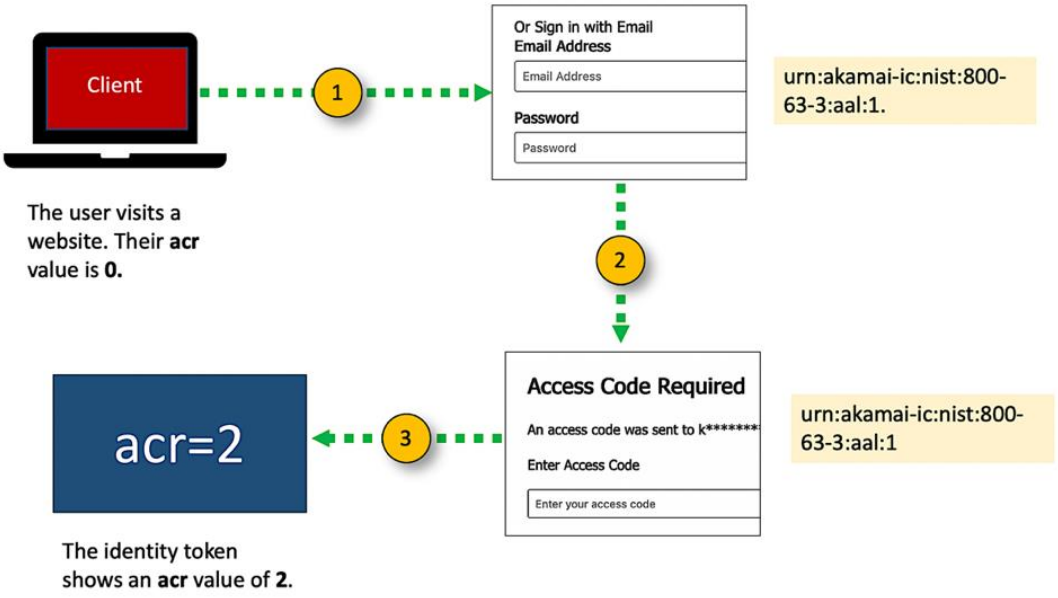

Рис. 2.10. Отримання параметра *acr_values*

Параметр acr_values

Заява *acr*, яку ми бачимо в маркері ідентифікації, повідомляє нам про рівень авторизації користувача. Якщо ми бачимо значення *acr 2*, ми знаємо, що користувач увійшов, використовуючи адресу електронної пошти та пароль, а потім пройшов двофакторну автентифікацію. Це дозволяє дізнатися поточний статус автентифікації користувача.

Але чому користувач пройшов автентифікацію, увійшовши в систему за допомогою адреси електронної пошти та пароля, а потім виконавши двофакторну автентифікацію? Чому він просто не увійшов в систему за допомогою адреси електронної пошти та пароля і не покінчили з цим?

Однією з причин цього може бути тип автентифікації, спеціально запитуваний у запиті авторизації користувача. Включивши параметр *acr_values* у запит на авторизацію, ми можемо вказати точний рівень автентифікації, який повинен мати користувач для входу. Наприклад, тут ми вимагаємо, щоб користувач пройшов автентифікацію за допомогою адреси електронної пошти та пароля, а потім пройшов двофакторну автентифікацію (рівень гарантії *urn:akamai-ic:nist:800-63-3:aal:2*).

У свою чергу, Hosted Login вимагатиме від користувача входу за допомогою адреси електронної пошти та пароля, а потім ініціювати процес двофакторної автентифікації. Наразі це єдиний спосіб отримати доступ до *urn:akamai-ic:nist:800-63-3:aal:2.*

У параметрі *acr_values* немає нічого складного: якщо ми знаємо дозволені рівні надійності, ми можемо використовувати цей параметр у своїх запитах авторизації. Просто майте на увазі, що всі претензії, на які посилається цей параметр, є «добровільними». Це означає, що такі претензії прийнятно мати, але вони не є обов’язковими: Hosted Login спробує надати запитуваний рівень авторизації, але цей рівень не гарантується. Ми можемо запитати рівень гарантії *urn:akamai-ic:nist:800-63-3:aal:2*, але ми не завжди його отримаємо.

3 ТЕХНОЛОГІЯ УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ТА ДОСТУПОМ КЛІЄНТІВ ДО ХМАРНИХ СЕРВІСІВ ОРГАНІЗАЦІЇ НА БАЗІ AKAMAI IDENTITY CLOUD

3.1. Порядок застосування рішення Akamai Identity Cloud

Як продукт керування інформацією та доступом клієнтів (CIAM), основна задача Akamai Identity Cloud полягає в тому, щоб дозволити користувачам створювати облікові записи у корпоративному додатку чи на веб-сайті, а потім мати можливість повернутися на цей веб-сайт чи додаток та увійти до свого облікового запису. Іншими словами, Akamai Identity Cloud відображає екрани входу, подібні до зображеного на рисунку 3.1.

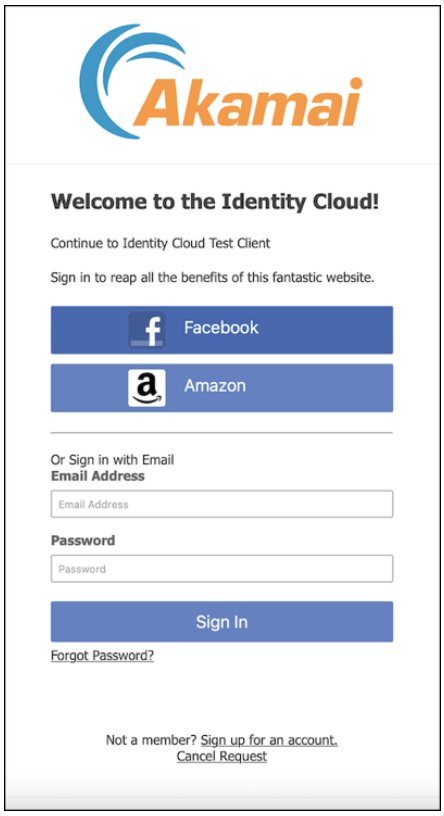

Рис. 3.1. Інтерфейс користувача Akamai Identity Cloud

Можливості рішення Akamai Identity Cloud [4]:

застосування широко використовувані та загальноприйняті стандарти, такі

як OAuth 2.0 і підключення OpenID, щоб переконатися, що процес входу та реєстрації є безпечним і безпечним;

надання дозволу користувачам входити на корпоративний сайт за допомогою Facebook, Twitter або практично будь-якого іншого соціального постачальника ідентифікаційних даних для входу;

надання додаткових функцій безпеки, наприклад двофакторну автентифікацію;

контроль над зовнішнім виглядом входу та реєстрації;

спрощення для користувачів доступу до своїх облікових записів і особистих даних і керування ними;

моніторинг активності на корпоративному веб-сайті чи в додатку, даючи фахівцям можливість помітити і зупинити аномальні ситуації (наприклад, будь-яку зловмисну діяльність), перш ніж вони стануть повномасштабною проблемою;

дозволяє переглядати детальні звіти про корпоративні веб-сайти та про те, хто (і коли, і звідки) насправді використовує ці сайти;

обмін даними з іншим програмним забезпеченням, наприклад із інструментом Customer Relations Manager.

Керування входом і реєстрацією користувачів

Рішення Akamai Identity Cloud дозволяє користувачам створювати облікові записи у корпоративному додатку чи на веб-сайті, входити в ці облікові записи та розпізнаватися як певний користувач (наприклад, *karim.nafir@mail.com*) і мати доступ до всього, на що *karim.nafir@mail.com* має право доступу. Щоб допомогти керувати логінами та реєстраціями, функція розміщеного входу Akamai Identity Cloud широко використовує як OAuth, так і OpenID Connect, пропонуючи підтримку для таких речей, як різні типи дозволів, різні типи відповідей і режимів, а також широкий спектр областей і претензій (включаючи спеціальні претензії) (рисунок 3.2).

Дозвіл користувачам використовувати соціальні логіни

Думка про необхідність створити ще один обліковий запис користувача та запам’ятати пароль ще одного облікового запису користувача може бути занадто

важкою для деяких людей, але це нормально.

```
https://v1.api.us.janrain.com/e0a70b4f-1eef-4856-bcdb-f050fee66aae/login/authorize
    ?client_id=8b875a65-6e88-4120-8656-c15603cedb9e
    &redirect_uri=https://oidc-playground.akamai.com/redirect_uri
    &scope=openid
    &code_challenge=kxVUGSgqy2xcDUneDJsTOXodk0cdVMMF-XjxRWW_00Y
    &code_challenge_method=S256
    &prompt=login
    &response_type=code
    &claims={"userinfo":{"preferred_username":null,"email":null}}
    &state=Iuuk7c94AClCWlFXuuVlhu6H34aSMonWwvMk4aHXWEQ
```

Рис. 3.2. OpenID Connect

Зрештою, Akamai Identity Cloud дозволяє користувачам реєструватися та входити за допомогою облікового запису, створеного в соціальних мережах, таких як Facebook, Twitter або Amazon. Таким чином, вам не потрібно турбуватися про нове ім’я користувача чи новий пароль: якщо ви пам’ятаєте, як увійти у Facebook, у вас усе буде добре (рисунок 3.3).

Рис. 3.3. Використання соціальних логінів клієнтами

Залежно від постачальника ідентифікаційної інформації, ми також можемо автоматично скопіювати дані з облікового запису входу в соціальну мережу до профілю користувача Akamai Identity Cloud нового користувача. Чи користувач уже ввів свою адресу, день народження та номер телефону в обліковому записі Facebook? Чудово: дані можна (за належної конфігурації та явної згоди користувача) скопіювати до його облікового запису Akamai Identity Cloud.

До речі, Akamai Identity Cloud підтримує близько 30 постачальників

ідентифікаційних даних для входу в соціальні мережі. Але що, якщо вони не підтримують постачальника ідентифікаційної інформації, якого ви хочете використовувати? Немає проблем: якщо цей постачальник використовує OAuth 2.0, OpenID Connect або SAML2, ми можемо використовувати можливості нашого спеціального постачальника для підключення до цього постачальника ідентифікаційних даних для входу в соціальні мережі.

Додавання додаткових заходів безпеки

Рішення Akamai Identity Cloud досить безпечне і надійне. Тим не менш, у наш час ніколи не завадить бути ще більш безпечним і безпечним. Маючи це на увазі, ми можемо легко застосувати додаткові заходи безпеки, щоб захистити облікові записи користувачів. Наприклад, ми можемо реалізувати двофакторну автентифікацію, щоб перешкодити хакерам, які якимось чином отримали ім'я користувача та пароль (рисунок 3.4).

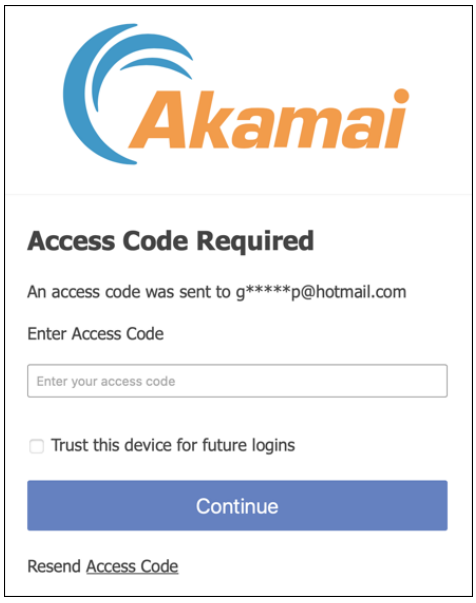

Рис. 3.4. Інтерфейс двофакторної автентифікації

Наявність пароля мало користі, якщо у нас також немає одноразового коду доступу з обмеженим терміном дії. Крім того, ми можемо застосувати вимоги до складності пароля, які не дозволять користувачам використовувати такі паролі, як пароль або 123456. Ми також можемо ввімкнути унікальний пароль, який

гарантує, що користувач не зможе «змінити» свій існуючий пароль на той самий пароль, який він використовує зараз. Цю функцію можна налаштувати для відстеження останніх 10 паролів користувача.

Якщо говорити про паролі, паролі Akamai Identity Cloud завжди зберігаються в зашифрованому форматі. Навіть адміністратори не можуть отримати доступ до пароля користувача.

Існує можливість Akamai забезпечити репутацію клієнта, яка визначає «оцінку ризику» клієнта на основі попередньої історії, пов'язаної з IP-адресою клієнта (тобто «Ця IP-адреса використовувалася раніше в відомих фішингових атаках. Нам повинні знадобитися два фактори автентифікації для цього користувача?»). Ми повинні згадати автентифікацію на основі ризиків і репутацію клієнта, тому що це ще два способи допомогти зберегти наш сайт і особисті дані наших користувачів у безпеці.

Налаштування користувацького досвіду

За умовчанням, коли ми вперше отримуємо доступ до розміщеного входу, ми побачимо екран входу з логотипом Akamai угорі, екран входу, який також використовує кольори Akamai, значок Akamai, термінологію та шрифти Akamai тощо. Правда, цілком можливо, що нам насправді не потрібен екран входу на тему Akamai. І це добре: Akamai Identity Cloud дає змогу легко змінити логотип, піктограму веб-сторінки чи текст, який використовується на екрані. Якщо ми хоч трохи розуміємося на CSS, ми можемо створити зовсім інший досвід входу (рисунок 3.5).

Можливість безпечно переглядати та керувати своїми особистими даними користувачам

Якщо ми керуємо додатком або веб-сайтом, ми маємо знати вимоги GDPR (Загальним регламентом захисту даних) Європейського Союзу та подібними ініціативами, розробленими для захисту конфіденційності користувачів і надання користувачам прав власності на дані, які ми збираємо та зберігаємо про них. Рішення Akamai Identity Cloud відповідає не лише GDPR, але й ISO 27001, ISO 27019, Критеріям довірчих послуг AICPA щодо безпеки, доступності, цілісності

обробки, конфіденційності.

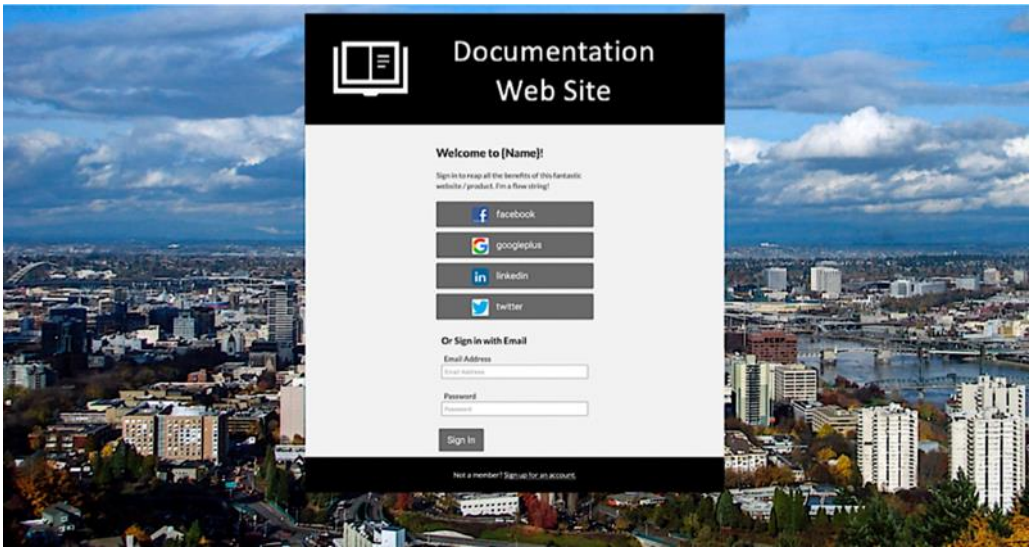

Рис. 3.5. Альтернативне розміщенння входу

Користувачі мають механізм для запиту копій своїх даних користувача, а також мають механізм для запиту на видалення своїх облікових записів і повного видалення даних користувачів із системи.

Крім того, Identity Cloud дозволяє легко налаштовувати дані, які ми збираємо та підтримуємо. Наприклад, за замовчуванням типи об’єктів Identity Cloud (тобто бази даних облікових записів користувачів) не мають способу відстежувати улюблений колір користувача чи його щасливе число. Ми кажемо, що у нас є вагома причина вимагати цю інформацію від користувачів. Потім надсилаємо запит: типи об’єктів можна змінити для зберігання будь-яких даних, які ми хочемо зберігати. І, як згадувалося раніше, екрани Akamai Identity Cloud можна легко змінити для запиту цих даних.

Видимість майже в реальному часі на своєму сайті

SIEM (Інформація про безпеку та керування подіями) це стандартний спосіб моніторингу, узагальнення та аналізу подій, які відбуваються на корпоративних веб-сайтах і у додатках. Крім усього іншого, використання подій SIEM і спеціального інструменту аналізу SIEM може виконувати такі дії, як постійний підрахунок скидання паролів користувача. Так, користувачі правомірно час від

часу скидають свої паролі. Однак несподівано велика кількість скидань пароля, які відбуваються одночасно, часто є ознакою порушення безпеки. Знову ж таки, назву лише один приклад: інструмент SIEM може сповіщати вас щоразу, коли кількість скинутих паролів починає перевищувати очікувану кількість скидань.

Слід також додати, що Akamai Identity Cloud надає лише «необроблені» події SIEM, текстові файли, які виглядають приблизно як показано на рисунку 3.6.


```
{
    "id":
    "message": {
        "app_id": "htb8fuhxnf8e38jrzub3c7pfrr",
        "client_id": "nmub5w3rru9k6rzupqaeb7bbwv6jn658",
        "endpoint_uri": "http://documentation.akamai.com/widget/traditional_signin.
jsonp",
        "event_type": "legacy_traditional_signin",
        "forward_headers": [
            {
                "name": "HTTP_X_FORWARDED_FOR",
                "value": "192.168.1.1, 192.168.1.2, 192.168.1.3"
            },
            {
                "name": "HTTP_X_FORWARDED_PROTO",
                "value": "http"            },
            {
                "name": "HTTP_X_FORWARDED_PORT",
                "value": "80"
            }
        ],
        "ip_address": "192.168.1.1",
        "origin": "https://login.documentation.akamai.com/",
        "user_agent": "Mozilla/5.0 (Android 8.1.0; Mobile; rv:68.0) Gecko/68.0 Fire
fox/68.0",
        "user_uuid": "437920f3-85dd-4cb7-ba8c-7025faeaid2c"
    },
    "msts": 1566206726081,
    "type:" "siem#legacy_traditional_signin"
}
```


Рис. 3.6. Формат даних для SIEM

Моніторинг за подіями користувачів

Неодмінно відбудуться певні події користувача, які становлять особливий інтерес для організації. Наприклад, припустімо, що у нас особлива подія, під час якої будь-кому, хто створить новий обліковий запис на в сайті, буде надіслано винагороду. У такому випадку нам потрібно отримувати сповіщення кожного разу, коли хтось створює обліковий запис, краще додати його до списку людей, яким буде надіслано винагороду.

Так само ми можемо отримувати сповіщення кожного разу, коли користувач натискає кнопку «Запитувати мої дані» у своєму профілі користувача. Таким

чином ми можете швидко зібрати та надіслати потрібні дані цьому користувачеві. Знати, скільки користувачів переходять у свій профіль користувача та змінюють свої імена по батькові, може бути не надто цікавим для нас. Знання того, скільки користувачів переходять до свого профілю користувача та змінюють свою згоду користувача з дозволу на заборону, може бути іншою історією.

Сервіс Webhooks v3 від Akamai Identity Cloud надає можливість отримувати сповіщення майже в реальному часі щоразу, коли відбувається певна подія користувача.

Перегляд та аналіз статистики сайту

Webhooks v3 це чудовий спосіб отримувати сповіщення кожного разу, коли відбувається певна подія користувача. Користувач щойно створив обліковий запис? Ось надходить сповіщення.

Немає нічого поганого в тому, щоб отримувати сповіщення щоразу, коли відбувається подія. Однак, якби це був єдиний спосіб отримати дані, ми ризикуємо пропустити ліс для дерев. Зрештою, замість того, щоб знати, що облікові записи користувачів було створено об 11:01, 11:02 та 11:03, ми могли б цікаво знати, скільки облікових записів було створено цього місяця, крапка. Можливо, нам буде цікаво дізнатися, як це порівняти з кількістю облікових записів, створених минулого місяця. І нам може бути цікаво дізнатися, виходячи з поточних тенденцій, скільки нових облікових записів може бути створено наступного місяця.

Щоб надати іншу точку зору на статистику корпоративного додатку чи веб-сайту, а також допомогти нам проаналізувати та зрозуміти цю статистику, клієнти Identity Cloud можуть використовувати Customer Insights, основний інструмент аналізу даних Identity Cloud. За замовчуванням Identity Cloud постачається з кількома «інформаційними панелями», які надають нам такі дані, як на рисунках 3.7 та 3.8.

Якщо стандартний набір інформаційних панелей не містить даних, які нас найбільше цікавлять, то Customer Insights дозволяє створювати власні інформаційні панелі, а також власні діаграми та графіки.

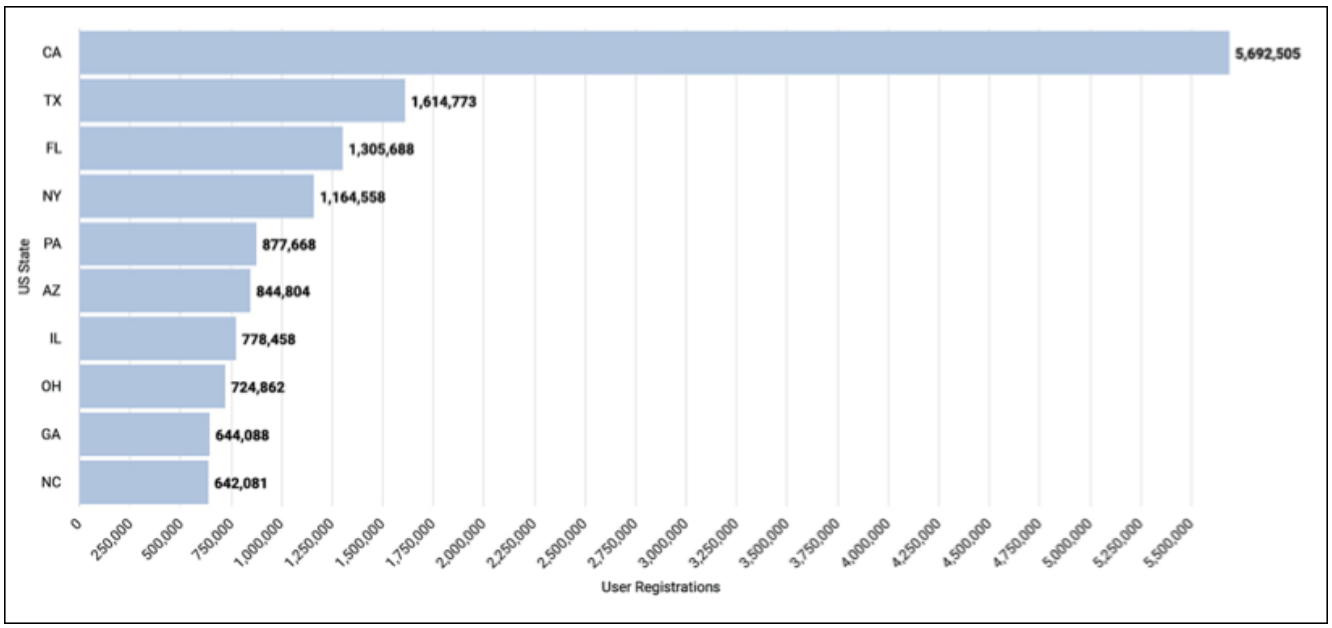

Рис. 3.7. Дані Customer Insights

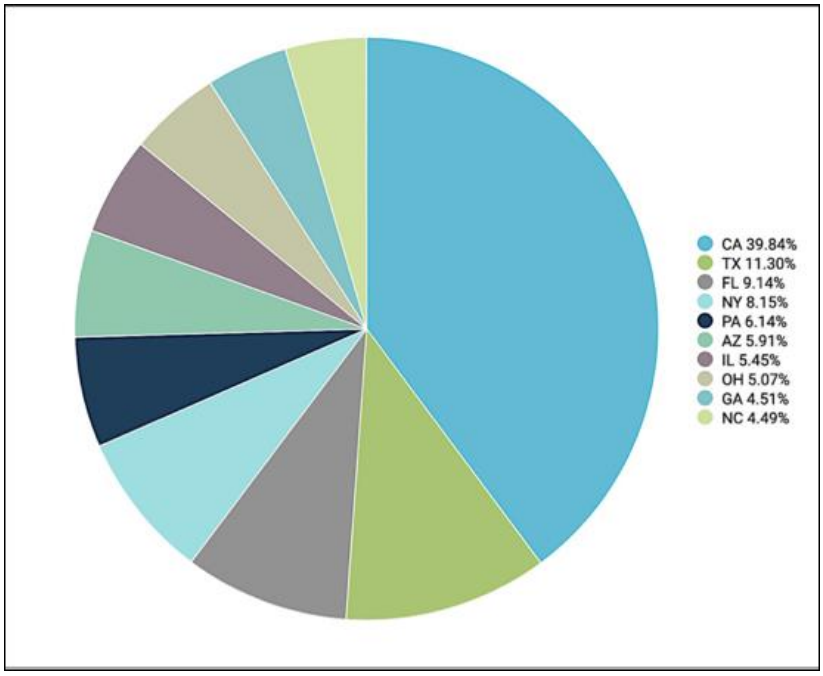

Рис. 3.8. Дані Customer Insights

Надання даних іншим платформам

Функція шини інтеграції дає нам можливість ділитися своїми даними користувача, скажімо, із програмним забезпеченням CRM. Наприклад, шину інтеграції можна налаштувати таким чином, що кожного разу, коли на нашому веб-сайті Identity Cloud створюється новий обліковий запис користувача, ця

інформація копіюється в Salesforce Marketing Cloud (рисунок 3.9)

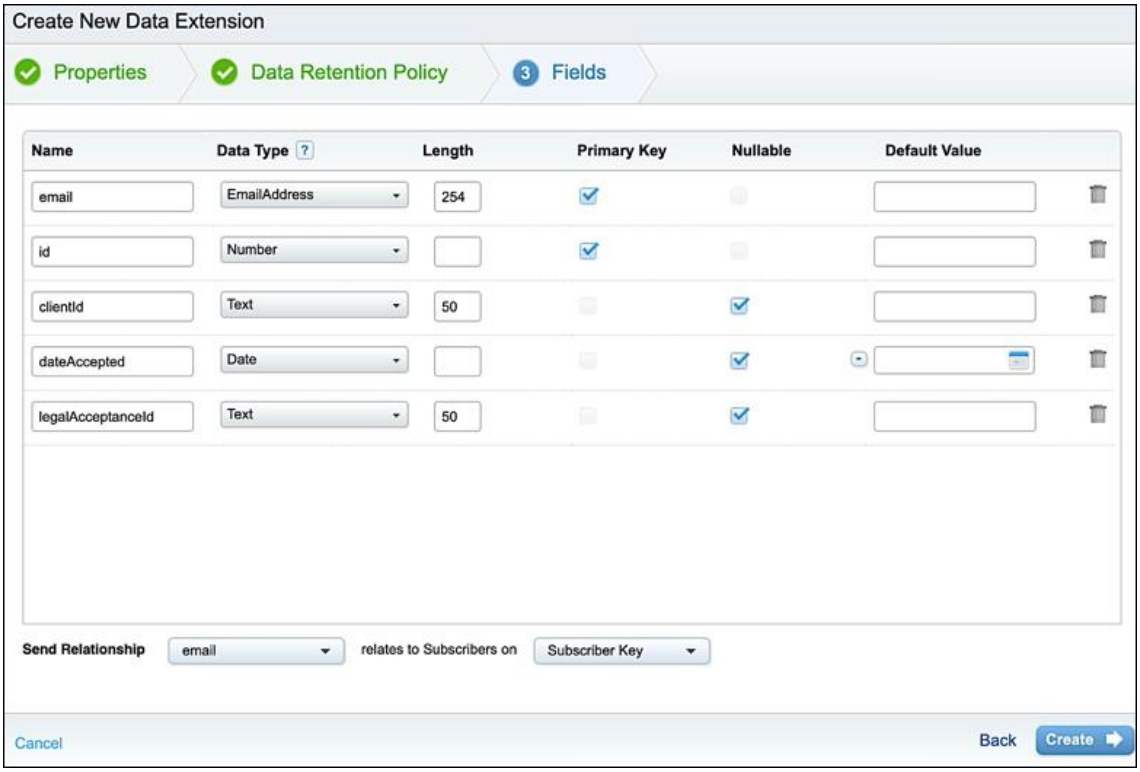

Рис. 3.9. Надання даних іншим платформам

Плавний перехід на Akamai Identity Cloud

За допомогою служби міграції даних Akamai Identity Cloud ми можемо перенести наявні облікові записи з поточної платформи до Akamai Identity Cloud (рисунок 3.10).

```
Starting the dataload import

        Loading data from sample_data.csv into the 'user' entity type

        Validating UTF-8 encoding and checking for Byte Order Mark

Labels: Total Success(S) | Total Fails(F) | Total Retries(R) | Success Rate(SR) | Average Reco

S:2 F:0 R:0 SR:100.0% AVG:362rec/m : 100%|


Starting the update process for the duplicated records


DATALOAD RESULTS
        [2] Total processed users

        [2] Import success. Number of new records inserted in database
        [0] Import failures


        [5] Total number of records in Entity Type [user] after execution
```

Рис. 3.10. Міграція даних Akamai Identity Cloud

Ця міграція включає не лише сам обліковий запис, але й усі пов’язані з ним дані, включаючи пароль користувача.

3.2. Технологія управління ідентифікацією та доступом клієнтів до хмарних сервісів організації на базі Akamai Identity Cloud

Необхідно відмітити, що Akamai Identity Cloud – це платформа програмного забезпечення як послуги (SaaS), яка допомагає компаніям керувати процесами ідентифікації клієнтів і керування доступом (CIAM). Його розроблено для захисту даних і додатків клієнтів і забезпечення глобальної доступності.

Розглянемо технологію забезпечення веб-сервісів через платформу Akamai.

Запит кінцевого користувача отримує доступ до граничного сервера Akamai, який є найближчим до кінцевого користувача. Якщо кінцевий користувач знаходиться, наприклад, в ЄС, периферійний сервер у ЄС відповість на запит.

Граничний сервер передає запит через платформу Akamai на вихідний сервер клієнта. На зворотному шляху до кінцевого користувача вихідний сервер надає веб-ресурси через платформу Akamai назад до кінцевого користувача.

Клієнт вибирає безпеку своїх веб-ресурсів. Для розумних веб-ресурсів Akamai рекомендує вибрати Akamai Enhanced TLS Platform для передачі.

На розширеній платформі TLS з’єднання TLS розривається для екземпляра Akamai на граничному сервері для виконання маршрутизації, зіставлення та перевірки безпеки. Одразу після цього з’єднання TLS відновлюється.

Клієнт визначає, кешуються/зберігаються веб-ресурси на граничних серверах чи ні.

Якщо веб-ресурси клієнта складаються з особистих даних, Akamai рекомендує вибрати конфігурацію без кешу для таких даних, щоб уникнути доступу до таких даних для будь-яких кінцевих користувачів, які мають доступ до веб-ресурсів клієнта (це і є ідея кешу).

У разі виявлення зловмисної діяльності на периферійному сервері запит блокується.

Якщо запити є законними, вони передаються через платформу Akamai.

Оскільки Akamai не знає, коли і де запит кінцевого користувача потрапляє на певний периферійний сервер, він не контролює, який сервер доставляє даний веб-ресурс або коли та де відбувається завершення TLS для даного веб-ресурсу.

Отже, за природою платформи Akamai дотримується принцип конфіденційності за проектом: якщо кінцевий користувач із ЄС запитує веб-ресурси клієнта, веб-ресурси та вбудовані персональні дані (якщо такі є) обробляються на Akamai сервері, розгорнутому в ЄС, за винятком кутових випадків, коли передача на серверах ЄС неможлива.

Завдяки понад 100 000 серверів Akamai, розгорнутих у регіоні ЄС, забезпечується швидка, надійна та безпечна доставка в регіоні за умовчанням.

Правила безпеки клієнта, правила Akamai та аналіз загроз Akamai застосовуються локально на граничному сервері.

Коли запит кінцевого користувача потрапляє на периферійний сервер, аналітика безпеки виконується на периферійному сервері:

передаються законні запити;

блокуються зловмисні запити.

Для законних запитів кінцевих користувачів, які знаходяться в ЄС, веб-ресурс клієнта обробляється в ЄС. Жодні дані не передаються за межі ЄС, за винятком кутових випадків.

Файли журналів підозрілих запитів передаються до США для аналізу систем безпеки Akamai, розгорнутих у США.

Відбувається обробка файлів журналу для цілей аналітики та підтримки обслуговування.

Identity Cloud – це служба керування ідентифікацією кінцевого користувача на додаток до веб-сервісів продуктивності Akamai [15].

Елементи персональних даних, що обробляються, стосуються особи кінцевого користувача, наприклад, ім'я, електронна пошта, адреса, номер телефону, вік, стать, історія покупок (наприклад, розмір взуття, бажана зубна паста).

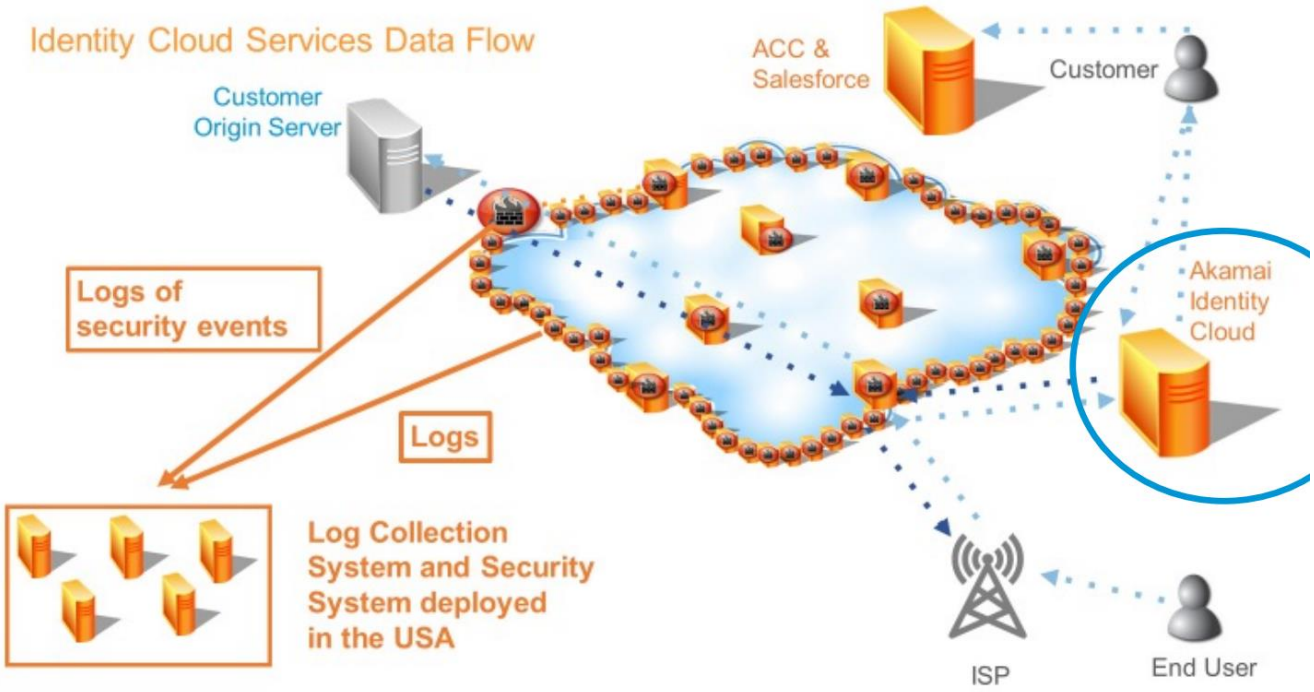

Рис. 3.11. Місце рішення Akamai Identity Cloud в платформі забезпечення веб-сервісів [15]

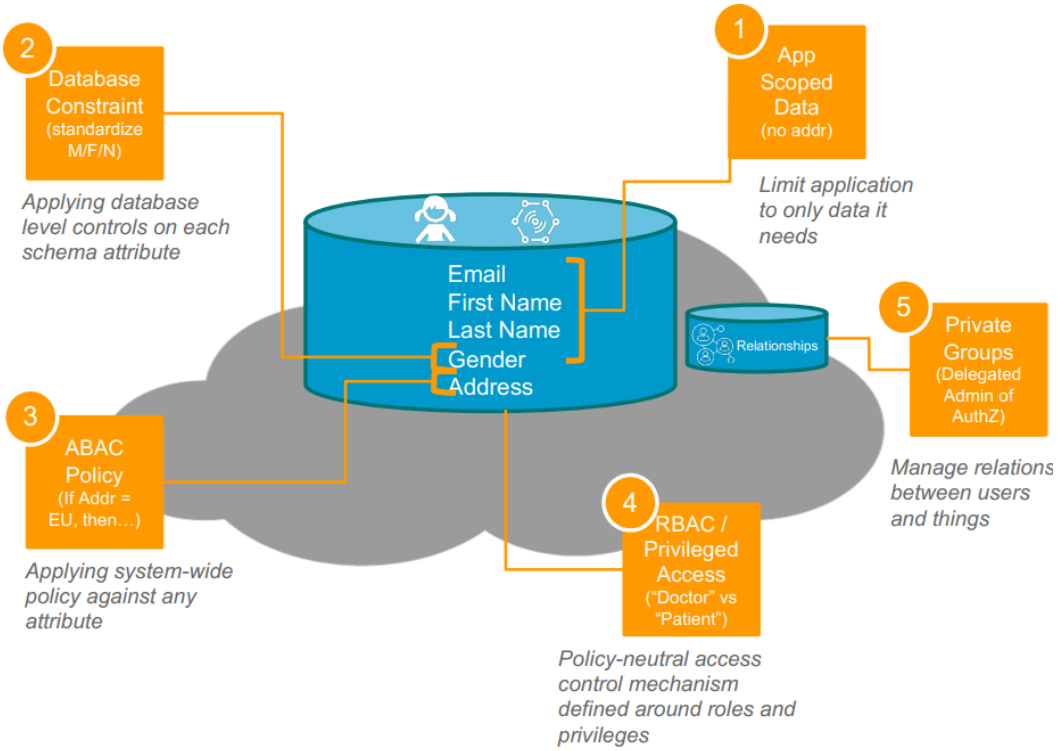

Рис. 3.12. Система забезпечення конфіденційності [15]

Елементи персональних даних збирає клієнт, а не Akamai. Akamai розміщує та захищає дані лише в Identity Cloud.

Identity Cloud працює на AWS як підпроцесор Akamai.

За допомогою конфігурації послуги клієнт визначає місце зберігання ідентифікаційних даних кінцевих користувачів (США, ЄС або APJ).

Служба продуктивності веб-сайтів Akamai забезпечує доступність і безпеку веб-ресурсів клієнтів через платформу Akamai (рисунок 3.11). Файли журналів обробляються.

Розроблена система забезпечення конфіденційності призвела до таких засобів контролю доступу (рисунок 3.12) [15]:

обмежений доступ до ідентифікаційних даних кінцевих користувачів для співробітників клієнта на основі ролей, обов'язків і типу/використання корпоративного додатка;

доступ лише за принципом необхідності мати;

точне керування до рівня окремих полів і стовпців запису даних;

доступ реєструється, і його можна легко відстежити у разі зловживання.

3.3. Рекомендації щодо управління ідентифікацією та доступом клієнтів до хмарних сервісів організацій

Для підвищення ефективності управління ідентифікацією та доступом клієнтів до хмарних сервісів організацій необхідно:

1. Зробити правильний вибір відповідних методів автентифікації. Першим кроком у впровадженні CIAM є вибір відповідних методів автентифікації. Це передбачає вибір правильного балансу між безпекою та зручністю.

Деякі з найпоширеніших методів автентифікації включають вхід на основі пароля, біометричний і соціальний вхід. Вибір методу залежить від характеру вашого бізнесу та конфіденційності даних, які ви обробляєте. Наприклад, якщо ви маєте справу з дуже конфіденційними даними, ви можете розглянути біометричну автентифікацію.

2. Забезпечити безпеку без шкоди для взаємодії з користувачем. Одним із найбільших завдань CIAM є забезпечення безпеки без шкоди для взаємодії з користувачем. Клієнти хочуть легкого, безперебійного доступу до корпоративних

послуг, але це не повинно відбуватися за рахунок безпеки.

Цього можна досягти шляхом впровадження таких заходів, як єдиний вхід (SSO) і вхід через соціальну мережу, які забезпечують безперебійну роботу користувача, зберігаючи при цьому високі стандарти безпеки.

3. Необхідно використовувати багатофакторну автентифікацію. Багатофакторна автентифікація (MFA) є ще однією важливою частиною CIAM. MFA вимагає від користувачів надати кілька доказів для підтвердження своєї особи. Це значно знижує ризик несанкціонованого доступу, оскільки навіть якщо один фактор скомпрометовано, зловмисникові все одно потрібні інші фактори, щоб отримати доступ.

Адаптивна MFA йде ще далі, коригуючи вимоги до автентифікації на основі рівня ризику транзакції. Наприклад, якщо користувач намагається ввійти з розпізнаного пристрою у знайомому місці, його можуть запитати лише пароль. Але якщо той самий користувач спробує ввійти з невідомого пристрою в іншій країні, його можуть попросити пройти додаткову перевірку.

4. Необхідно CIAM інтегрувати з існуючими системами. Ще один важливий момент при впровадженні CIAM – інтеграція з існуючими системами. Корпоративне рішення CIAM повинно легко інтегруватися з наявною інфраструктурою, включаючи систему управління взаємовідносинами з клієнтами (CRM), інструменти автоматизації маркетингу та інші бізнес-додатки.

Ця інтеграція дозволяє використовувати дані з корпоративного рішення CIAM для всього бізнесу, покращуючи залучення клієнтів, персоналізацію та загальну ефективність бізнесу.

5. Необхідно проводити регулярний моніторинг і аудит. Регулярний моніторинг і аудит мають вирішальне значення для забезпечення ефективності корпоративного рішення CIAM. Це передбачає відстеження всіх запитів на доступ, успішних і невдалих входів, а також будь-яких змін у профілях користувачів.

Відстежуючи ці події, ви можете швидко виявити будь-яку підозрілу активність і негайно вжити заходів. Регулярні перевірки також можуть допомогти

фахівцям виявити будь-які вразливі місця у корпоративній системі та вжити заходів для їх усунення.

6. Важливо дотримуватися нормативних вимог міжнародних стандартів та вітчизняних норм. Нарешті, дотримання нормативних вимог має вирішальне значення для автентифікації CIAM. Як згадувалося раніше, у різних країнах діють різні закони про конфіденційність. Таким чином, корпоративне рішення CIAM має бути в змозі впоратися з цими варіаціями та забезпечити відповідність.

Це передбачає регулярне оновлення корпоративної політики конфіденційності, отримання необхідної згоди користувачів і забезпечення відповідних заходів захисту даних. Недотримання вимог може призвести до юридичних санкцій і завдати шкоди репутації бренду.

ВИСНОВКИ

В роботі досліджено проблему управління ідентифікацією та доступом клієнтів до хмарних сервісів організацій, визначено його мету та завдання. Організації використовують рішення ідентифікації клієнтів і керування доступом, щоб контролювати доступ до загальнодоступних веб-сайтів і хмарних інформаційних ресурсів. Рішення CIAM полегшують клієнтам реєстрацію та вхід у онлайн-додатки та служби. Вони допомагають забезпечити конфіденційність даних і захистити від крадіжки особистих даних та інших видів шахрайства та зловживань. Такі рішення дозволяють клієнтам легко керувати своїми профілями облікових записів і налаштуваннями безпеки самостійно.

Визначено існуючі підходи до управління ідентифікацією та доступом клієнтів до хмарних сервісів організацій. Рішення управління ідентифікацією та доступом клієнтів до хмарних сервісів організацій пропонують набір можливостей для безпечного й ефективного керування ідентифікацією клієнтів і доступом. Основні функції включають реєстрацію користувача, автентифікацію, авторизацію, єдиний вхід, багатофакторну автентифікацію, перевірку ідентифікації, керування згодою та налаштуваннями, а також керування профілями користувачів.

Проаналізовано методи та засоби управління ідентифікацією та доступом клієнтів до хмарних сервісів організації на базі Akamai Identity Cloud. Визначено призначення, основні функції та склад рішення Akamai Identity Cloud. Рішення CIAM зазвичай надаються як хмарні служби, які розміщуються та керуються надійною третьою стороною для максимальної простоти, гнучкості та масштабованості. Необхідно підкреслити, що збираючи та обробляючи дані клієнтів, організації повинні дотримуватися багатьох правил захисту даних і конфіденційності. Рішення Akamai Identity Cloud дозволяє впоратися з цими проблемами.

На основі досліджень проведених в роботі запропоновано порядок

застосування технології управління ідентифікацією та доступом клієнтів до хмарних сервісів організації на базі Akamai Identity Cloud: порядок керування входом і реєстрацією користувачів, порядок надання дозволів користувачам використовувати соціальні логіни, порядок додавання додаткових заходів безпеки та інші.

Розроблено рекомендації фахівцям з кібербезпеки щодо управління ідентифікацією та доступом клієнтів до хмарних сервісів організацій.

Таким чином, правильна реалізація технології управління ідентифікацією та доступом клієнтів до хмарних сервісів має забезпечити ефективний захист корпоративних ресурсів та кібербезпеку інформаційної системи організації.

ПЕРЕЛІК ПОСИЛАНЬ

1. 2024 Imperva Bad Bot Report. URL: https://www.imperva.com/resources/resource-library/reports/2024-bad-bot-report/

2. What is Customer Identity and Access Management (CIAM)? CyberArk. URL: https://www.cyberark.com/what-is/ciam/

3. Global Compliance – Customer: Reference Architecture. Akamai. URL: https://www.akamai.com/resources/reference-architecture/global-compliance-customer

4. How Identity Cloud works. Akamai. URL: https://techdocs.akamai.com/identity-cloud/docs/an-introduction-to-identity-cloud

5. Identity Cloud: Product Brief. Akamai. URL: https://www.akamai.com/resources/product-brief/identity-cloud

6. What is CIAM? Benefits, Challenges, Use Cases. Customer Identity Access Management, August 1, 2024. URL: https://www.infisign.ai/blog/what-is-ciam-benefits-challenges-use-cases

7. Razi Chaudhry. A Guide to Key CIAM Capabilities and Implementation Blueprints. Medium, Jun 9, 2024. URL: https://medium.com/@razi_chaudhry/a-guide-to-key-ciam-capabilities-and-implementation-blueprints-ciam-part-4-3416bfb512d6

8. Identity & Access Management. NIST. URL: https://www.nist.gov/identity-access-management

9. Paul A. Grassi, Michael E. Garcia, James L. Fenton. Digital Identity Guidelines. NIST Special Publication 800-63-3. https://doi.org/10.6028/NIST.SP.800-63-3

10. 2024 State of Multicloud Security Report. Microsoft Security. URL: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/2024-State-of-Multicloud-Security-Risk-Report.pdf

11. Mirren McDade, Craig MacAlpine. The Top 8 Customer Identity And Access Management (CIAM) Solutions. Expert Insights. Last updated on Jun 24, 2024. URL: https://expertinsights.com/insights/top-customer-identity-and-access-management-ciam-

solutions/

12. Privilege Cloud architecture. CyberArk. URL: https://docs.cyberark.com/privilege-cloud-standard/latest/en/content/privilege%20cloud/privcloud-detailed-architecture.htm

13. Aaron Smalser. Inbound SCIM for Okta Customer Identity Cloud is now Generally Available. Okta, July 19, 2024. URL: https://www.okta.com/blog/2024/07/inbound-scim-for-okta-customer-identity-cloud-is-now-generally-available/

14. Azure AD B2C. ALIF Consulting, Mar 20, 2022. URL: https://www.alifconsulting.com/post/azure-ad-b2c

15. Power and protect life online. Akamai. URL: https://www.akamai.com/site/en/documents/akamai/2022/akamai-services-data-flows-risks-2022-06-14.pdf

16. Компанець Олександр Сергійович. Технологія управління ідентифікацією та доступом клієнтів за допомогою Akamai Identity Cloud. Всеукраїнська наукова конференція «Актуальні проблеми кібербезпеки». Державний університет інформаційно-комунікаційних технологій. 25 жовтня 2024. Тези доповідей. С. 93-96. URL: https://dut.edu.ua/uploads/p_2121_20358827.pdf.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)