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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Засоби ідентифікації користувачів до інформаційної системи організації»

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

_____ Владислав ПРАВДИВИЙ
(підпис)

Виконав: здобувач вищої освіти групи БСД-42
ПРАВДИВИЙ Владислав
(прізвище, ім'я)

Керівник ЧУМАК Надія
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент д.е.н., проф.ЛЕГОМІНОВА Світлана
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IAM – Identity and Access Management

SSO – Single Sign-On

ZTNA – Zero Trust Network Acces

ZT – Zero Trust

ZTA – Zero Trust Architecture

ВСТУП

Актуальність дослідження. Управління та ідентифікацією та доступом є процесом, який забезпечує належний доступ потрібних людей до потрібних ресурсів і запобігання доступу неавторизованих користувачів. Автентифікація — процес визначення користувачів, за яких вони себе видають — є одним із перших кроків у захисті даних, мереж і програм.

Вимога від користувачів надати та підтвердити свою особу додає рівень безпеки між зловмисниками та конфіденційними даними. Завдяки автентифікації IT-групи можуть застосовувати принцип найменших привілеїв, щоб обмежити те, що можуть бачити співробітники. Середньостатистичний працівник, наприклад, не потребує доступу до фінансів компанії, а кредиторська заборгованість не потребує торкатися проектів розробників.

Для такого розподілу працівників організації повинні виористовувати відповідні моделі доступу, які дозволять фахівцям з кібербезпеки спростити надання відповідних дозволів користувачам інформаційної системи організації для доступу для відповідних ресурсів.

У зв’язку зі збільшенням кількості атак на інформаційні системи облікові дані користувачів інформаційної системи організації повинні бути захищені та постійно бути під контролем. Використання сучасних засобів ідентифікації дозволяють управляти користувачами та надають можливості відслідковувати дії користувачів.

Отже, для ідентифікації користувачів інформаційної системи організації, необхідно впроваджувати комплексний підхід і використовувати сучасні платформи надання послуг з використання засобів ідентифікації.

Об’єкт дослідження – ідентифікація користувачів інформаційної системи.

Предмет дослідження – засоби ідентифікації користувачів інформаційної системи.

Мета роботи розробити варіант застосування засобів ідентифікації

користувачів інформаційної системи та рекомендації щодо їх застосування.

Наукові завдання:

дослідити сутність проблеми ідентифікації користувачів інформаційної системи;

проаналізувати основні підходи щодо впровадження заходів ідентифікації користувачів інформаційної системи;

проаналізувати існуючі рішення, які використовують засоби ідентифікації користувачів інформаційної системи;

проаналізувати засоби ідентифікації користувачів інформаційної системи на базі CyberArk Identity Security Platform;

запропонувати варіант впровадження заслбів ідентифікації користувачів інформаційної системи на базі CyberArk Identity Security Platform;

розробити рекомендацій щодо застосування засобів ідентифікації користувачів інформаційної системи.

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

Практичне значення одержаних результатів: розроблено рекомендації щодо застосування методів ідентифікації користувачів інформаційної системи та розроблено рекомендації фахівцям з кібербезпеки щодо їх реалізації.

1 АНАЛІЗ ПРОБЛЕМИ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ІНФОРМАЦІЙНОЇ СИСТЕМИ

1.1. Аналіз необхідності ідентифікації користувачів інформаційної системи

Ідентифікація користувачів є важливою складовою інформаційної безпеки організацій. Користувачі повинні проходити автентифікацію, коли щодня отримують доступ до своїх комп'ютерних систем на роботі чи вдома. Ідентифікація це процес контрольованого доступу до ресурсів за допомогою автентифікації, авторизації та обліку [1].

Ідентифікація користувача або ідентифікатор користувача — це унікальний ідентифікатор для визначення користувачів програмних систем, веб-сайтів або будь-якого загального ІТ-середовища. Для будь-якої ІТ-системи важливо розрізняти користувачів, які отримують до неї доступ або використовують її. Ідентифікатор користувача особливо зручний для входу на веб-сайт, у програму чи онлайн-сервіс. Це може бути ім'я користувача, номер рахунку або адреса електронної пошти [2].

Ідентифікатор користувача є одним із широко використовуваних методів автентифікації, популярних в Інтернеті, програмах і програмному забезпеченні. Кожен користувач має унікальний ідентифікатор, який відрізняє його від інших користувачів без шкоди для конфіденційності користувачів.

Зазвичай ідентифікатор користувача додається разом із паролем. Кінцевий користувач повинен правильно надати ці два записи, щоб отримати доступ до системи чи програми. Крім того, системні адміністратори використовують ідентифікатори користувачів для призначення дозволів, відстеження дій користувачів і керування загальною роботою певної системи, мережі чи програми.

У більшості цифрових транзакцій ідентифікація є етапом, на якому користувачі підтверджують свою особу, надаючи ім'я, адресу електронної пошти,

номер телефону або ім’я користувача [3].

Ідентифікація є першим кроком у підтвердженні особи людини і має відбутися перед автентифікацією та авторизацією. Користувачі також можуть надати додаткову інформацію, як-от державну фотографію, ідентифікаційний код або номер соціального страхування, щоб додатково ідентифікувати себе.

Ідентифікація відбувається на етапі початкового налаштування облікових записів і сервісів. Ім’я користувача та пароль зазвичай ідентифікують особу під час кожного доступу до цього облікового запису чи служби.

Однак у цифровому середовищі може бути складно підтвердити ідентифікацію просто шляхом отримання особистої інформації, імен користувачів і паролів. Викраденого гаманця або зламаного облікового запису електронної пошти також достатньо, щоб хтось спробував викрасти особистість.

Враховуючи ці ризики, ідентифікація є лише першим кроком до встановлення базової лінії для процесу автентифікації.

Автентифікація вимагає від користувачів довести, що вони все ще є тією особою, за яку себе видали на етапі ідентифікації.

У 2021 році FTC отримала понад 2,8 мільйона повідомлень про шахрайство, що призвело до збитків на суму понад 5,8 мільярда доларів. Якби ідентифікація була єдиною перешкодою між доступом до облікового запису чи системи, випадки шахрайства та крадіжки особистих даних були б ще більш поширеними. Автентифікація забезпечує рівень захисту, окрім ідентифікації, щоб допомогти користувачам захистити свої облікові записи та особистість.

Після базової ідентифікації автентифікація ініціює збіг між попередньо наданою інформацією користувача. Системи автентифікації все частіше запитують одноразовий код підтвердження, надісланий на адресу електронної пошти або номер телефону, навіть якщо надані користувачем дані та збережена інформація збігаються. Авторизація вимагає як ідентифікації, так і автентифікації.

Автентифікація — це процес, за допомогою якого користувач установлює свою особу під час доступу до мережевої програми чи служби. На етапі ідентифікації сервер отримує інформацію про особу користувача, після чого сервер

запитує автентифікацію або доказ того, що користувач є тим, за кого себе видає. Кілька процесів ідентифікації вважають комбінацію імені користувача та пароля ефективним процесом автентифікації.

На жаль, більшість людей не розуміють значення ідентифікації та автентифікації.

Таким чином, хоча ідентифікація є першим кроком у більшості онлайн-транзакцій, вона сама по собі не гарантує безпеку. Необхідна подальша автентифікація для підтвердження ідентичності, а потім авторизація для надання відповідних прав доступу. Спершу користувач заявляє, хто він є (ідентифікація), але система не може просто повірити йому на слово. Потрібен механізм, щоб довести цю заяву (автентифікація). Лише після цього система може вирішити, до яких ресурсів користувач має доступ (авторизація).

Автентифікація стає першим кроком у покращенні безпеки, враховуючи зростаючі вимоги до неї. Основна робота автентифікації полягає в тому, щоб керувати ідентифікацією користувачів і надавати їм відповідний контроль доступу для безперебійної роботи та безпеки. Індивідуальна автентифікація не повинна обмежуватися іменами користувачів і паролями. Єдиний вхід (SSO), багатофакторна автентифікація (MFA), ініціалізація , адаптивна автентифікація та інші засоби керування ідентифікацією та доступом (IAM) розширюють можливості стандартної автентифікації [4].

Розглянемо детально що таке автентифікація.

Автентифікація – це процес ідентифікації користувачів, які запитують доступ до системи, мережі, сервера, програми, веб-сайту або пристрою. Основна мета автентифікації — переконатися, що користувач є тим, за кого себе видає. Користувач А, наприклад, має доступ лише до відповідної інформації та не може бачити особисту інформацію користувача Б. Неавторизовані користувачі не можуть отримати доступ до конфіденційних даних за допомогою автентифікації користувача. Автентифікація покращує безпеку, дозволяючи будь-якому адміністратору організації керувати ідентифікацією та доступом окремого користувача. Основною автентифікацією, яка використовується для перевірки

ідентифікації та контролю доступу, є ім’я користувача та пароль, а також різні типи методів автентифікації, які ми розглянемо далі [4].

У сучасному сучасному світі немає жодної організації, системи, мережі, веб-сайту чи сервера, які б не потребували певної форми автентифікації. Якщо ні, вони піддають себе ризику атак, які можуть призвести як мінімум до незаконного привласнення їхніх ресурсів і конфіденційних даних. Одна помилка може стати доступною для даних вашої організації кіберзлочинцям, оскільки вони завжди готові за допомогою різноманітної кіберзброї, як-от (фішинг, витік даних, спуфінг тощо). Якщо система автентифікації не відповідає вимогам, вони можуть швидко отримати доступ і викрасти інформацію.

Ідентифікація користувачів відіграє важливу роль у забезпеченні кібербезпеки.

Ефективна ідентифікація користувачів є критично важливою для забезпечення кібербезпеки інформаційної системи організації. Ідентифікація є першою лінією захисту, яка запобігає несанкціонованому доступу до інформаційних систем. Ідентифікатор користувача є вашою ідентифікацією, і саме він пов'язує користувача з його діями в системі. Унікальний ідентифікатор користувача є основою для контролю доступу та застосування політик безпеки. Багато онлайн-сервісів, включаючи банківські операції, електронну пошту та соціальні мережі, потребують ідентифікації користувачів для надання послуг та захисту даних.

Ідентифікація користувачів покращує видимість мережевої активності на рівні користувачів, а не лише IP-адрес. Це дозволяє контролювати використання додатків та зменшує адміністративні зусилля, пов'язані зі змінами користувачів. Крім того, ідентифікація підтримує принцип найменших привілеїв, надаючи користувачам лише той доступ, який необхідний для виконання їхніх обов'язків.

Отже, ефективна ідентифікація є критично важливою не лише для контролю доступу, але й для забезпечення підзвітності та видимості дій користувачів, що є ключовими елементами кібербезпеки. Без чіткої ідентифікації неможливо відстежити, хто саме здійснив певну дію в системі. Це ускладнює розслідування

інцидентів безпеки та застосування відповідних заходів контролю.

Наведемо нормативні визначення ідентифікації користувачів на прикладі NIST [5, 6].

Національний інститут стандартів і технологій (NIST) визначає ідентифікатор користувача як унікальний символ або рядок символів, що використовується інформаційною системою для ідентифікації конкретного користувача.10 NIST SP 800-171 вимагає ідентифікації системних користувачів, процесів, що діють від імені користувачів, та пристроїв. Цей стандарт також підкреслює необхідність унікальної ідентифікації та автентифікації системних користувачів та пов'язання цієї ідентифікації з процесами, що діють від їх імені. За певних обставин, таких як зміна ролей або облікових даних, NIST рекомендує повторну автентифікацію користувачів.

Ці нормативні документи, такі як стандарти NIST, підкреслюють важливість унікальної ідентифікації користувачів як фундаментального контролю безпеки. Вони встановлюють вимоги до організацій щодо впровадження надійних процесів ідентифікації, що є необхідним для захисту інформаційних систем та даних.

Перейдемо до огляду статистики та тенденцій щодо витоків інформації у 2023-2025 роках.

Прогнозується, що глобальна вартість кіберзлочинності сягне 10,5 трильйона доларів США до 2025 року, зростаючи на 15 відсотків щорічно [5-6]. У 2023 році було зафіксовано значне зростання кількості публічно повідомлених витоків даних порівняно з 2022 роком.22 Велика кількість осіб постраждала від витоків даних як у 2023, так і у 2024 роках.22 У 2024 році спостерігалося збільшення кількості повідомлень про витоки даних, хоча загальна кількість інцидентів дещо зменшилася.23 Середня вартість витоку даних також зросла у 2023 та 2024 роках.25 Ця статистика чітко показує зростаючу загрозу витоків інформації, що підкреслює необхідність посилення заходів безпеки, включаючи процеси ідентифікації користувачів. Збільшення як кількості, так і вартості витоків даних свідчить про те, що кіберзлочинці стають дедалі успішнішими, а наслідки атак – серйознішими.

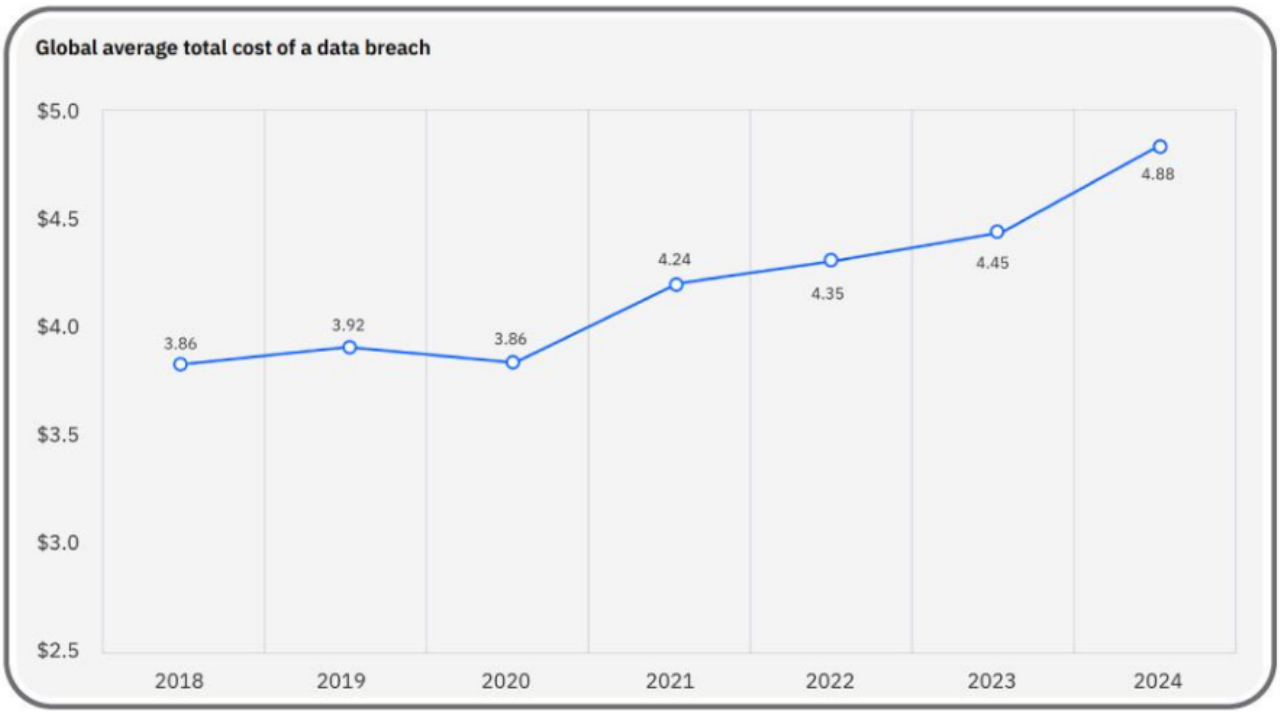


Рис.1.1. Вартість витоку даних

Аналіз звітів про кібератаки, пов'язані зі скомпрометованими обліковими даними показав, що 2022 році скомпрометовані облікові дані були найпоширенішим початковим вектором атаки. Високий відсоток витоків даних у 2023 та 2024 роках був пов'язаний з використанням викрадених облікових даних. Спостерігалося збільшення кількості інцидентів, де легітимні інструменти використовувалися для крадіжки облікових даних. Витоки, пов'язані зі скомпрометованими обліковими даними, мали тривалий час виявлення та локалізації. У 2024 році значна кількість кібератак призвела до витоків через те, що зловмисники отримали доступ до мереж, використовуючи скомпрометовані облікові записи, які не були захищені багатофакторною автентифікацією.. Зловмисники також використовували шкідливе програмне забезпечення для крадіжки облікових даних, що дозволяло їм обходити MFA. Скомпрометовані облікові дані залишаються однією з основних причин витоків інформації, а зловмисники постійно вдосконалюють свої методи їх отримання та використання. Незважаючи на впровадження MFA, атаки на облікові дані залишаються ефективними, що свідчить про необхідність комплексного підходу до захисту.

У багатьох випадках витоки інформації у 2023-2024 роках були спричинені

слабкими механізмами ідентифікації. Використання слабких або стандартних паролів стало причиною успішних атак. Також були зафіксовані вразливості, пов'язані з обходом автентифікації. Неналежне керування обліковими даними також призводило до витоків. Атаки методом "грубої сили" були успішними проти систем з недостатнім захистом. Крім того, зловмисники використовували вразливості API через слабку безпеку облікових даних. Слабкі механізми ідентифікації, такі як використання простих паролів або відсутність належного захисту від атак, роблять інформаційні системи вразливими до компрометації. Якщо системи ідентифікації не відповідають сучасним вимогам безпеки, зловмисникам стає значно легше отримати несанкціонований доступ.

У 2024 році велика кількість витоків даних сталася через відсутність багатофакторної автентифікації (MFA), яких можна було б уникнути за її наявності.23 MFA є ефективним способом запобігання використанню викрадених облікових даних. Однак зловмисники навчилися обходити MFA через викрадення файлів cookie сеансу. Також були зафіксовані атаки на слабкі реалізації MFA, такі як використання SMS-кодів, які можуть бути перехоплені. Відсутність або неналежне впровадження MFA є значною вразливістю, яку активно експлуатують зловмисники для отримання несанкціонованого доступу. Хоча MFA значно підвищує рівень безпеки, його неправильна реалізація або використання вразливих методів може звести нанівець його переваги.

Розглянемо типи атак, які використовують слабкі сторони процесів ідентифікації (рис.1.2).

Фішинг є одним з найпоширеніших методів кібератак, спрямованих на крадіжку облікових даних. Це атака, яка намагається викрасти ваші гроші або вашу особистість, змушуючи вас розкрити особисту інформацію, таку як номери кредитних карток, банківську інформацію або паролі, на веб-сайтах, які видають себе за легітимні. Кіберзлочинці зазвичай видають себе за авторитетні компанії, друзів або знайомих у підробленому повідомленні, яке містить посилання на фішинговий веб-сайт. Фішинг облікових даних відповідає майже за 70% усіх кібератак на основі електронної пошти.

Рис.1.3. Типи атак, які використовують слабку ідентифікацію

Атаки методом "грубої сили" (Brute-force) - це спроба отримати доступ до системи шляхом систематичного перебору різних паролів, поки не буде знайдено правильний набір облікових даних. Зловмисники використовують автоматизовані інструменти для швидкого тестування різних комбінацій паролів, експлуатуючи слабкі паролі та системи, які не мають захисних заходів, таких як блокування облікових записів або обмеження швидкості. Хмарні середовища стикаються з додатковими ризиками через атаки "грубої сили" на API-ключі та відкриті адміністративні інтерфейси. Атаки "грубої сили" в своїй найпростішій формі перебирають кожну можливу комбінацію символів, поки не буде знайдено пароль або ключ шифрування рис.1.3. Більш складні версії намагаються швидше знайти відповідність, починаючи з простих і часто використовуваних паролів зі списку, а потім вдаючись до вичерпного пошуку.

Рис.1.3. Атаки методом "грубої сили"

Атаки "грубої сили" можуть бути спрямовані не лише на традиційні сторінки входу. Вони можуть атакувати API хмарних сервісів, використовуючи автоматизовані скрипти для багаторазового вгадування API-ключів або облікових даних. Вони також можуть використовуватися для вгадування облікових даних для входу в бази даних або навіть облікових записів адміністраторів хмарних сервісів, надаючи зловмисникам глибокий доступ до хмарної інфраструктури. Зловмисники використовують їх, щоб отримати несанкціонований доступ до облікових записів та систем, підвищити привілеї, змінити налаштування або вимкнути засоби контролю безпеки, викрасти дані, встановити шкідливе програмне забезпечення або використовувати скомпрометовані облікові записи як плацдарм для подальших атак.

Крадіжка облікових даних (Credential Theft) - це процес викрадення облікових даних. Зловмисники зазвичай використовують фішинг для крадіжки облікових даних, оскільки це досить дешева та надзвичайно ефективна тактика. Ефективність фішингу облікових даних залежить від взаємодії з людиною, на відміну від шкідливого програмного забезпечення та експлойтів, які покладаються на слабкі місця в захисті безпеки. Корпоративна крадіжка облікових даних зазвичай є цілеспрямованою діяльністю. Зловмисники переглядають сайти соціальних мереж, такі як LinkedIn, у пошуках конкретних користувачів, чиї облікові дані нададуть доступ до важливих даних та інформації. Фішингові електронні листи та

веб-сайти, які використовуються для корпоративної крадіжки облікових даних, є набагато складнішими, ніж ті, що використовуються для крадіжки облікових даних споживачів. Зловмисники докладають значних зусиль, щоб ці електронні листи та веб-сайти виглядали майже ідентично легітимним корпоративним додаткам та комунікаціям. Саме на цьому етапі атак, що базуються на облікових даних, навчання з підвищення обізнаності про безпеку відіграє роль першої лінії захисту. Після того, як зловмисник отримує облікові дані користувача та паролі, він може продати їх у кіберзлочинному підпіллі або використовувати їх для компрометації мережі організації, обходячи всі заходи безпеки, щоб не допустити зловмисника, переміщатися в межах мережі та викрадати дані.

Атаки з використанням "начинки" облікових даних (Credential Stuffing) - це тип кібератаки, при якій викрадені імена користувачів та паролі використовуються для отримання несанкціонованого доступу до багатьох веб-сайтів, використовуючи поширену практику повторного використання паролів для здійснення шахрайських дій. Оскільки 78% користувачів повторно використовують один і той же пароль на кількох сайтах, "начинка" облікових даних є загрозою для кожної організації з онлайн-акаунтами. Для здійснення кібератаки з використанням "начинки" облікових даних хакери використовують викрадені облікові дані для спроби доступу до різних сайтів, використовуючи такі інструменти, як ботнети та ротація IP-адрес, щоб уникнути виявлення. Після входу в систему зловмисники можуть ініціювати захоплення облікового запису, перетворюючи один викрадений обліковий запис на набагато більшу загрозу. Списки викрадених паролів можуть містити сотні мільйонів імен користувачів та паролів і часто доступні зловмисникам за відносно невелику суму. На цьому етапі кіберзлочинці використовують спеціальні комп'ютерні програми, звані ботами, щоб одночасно намагатися увійти на багато веб-сайтів. Ці автоматизовані програми можуть тестувати тисячі паролів щохвилини.

Також загрозу несуть поширені вразливості в системах ідентифікації.

Однією з найпоширеніших вразливостей в системах ідентифікації є використання слабких та легко вгадуваних паролів. Багато користувачів досі

обирають паролі, які легко вгадати, такі як "123456" або "Qwerty123". Крім того, часто використовуються особиста інформація або загальновідомі слова, такі як імена, дати народження або назви домашніх тварин. Повторне використання паролів на різних платформах також є серйозною проблемою. Недостатня складність паролів робить їх легкою ціллю для атак методом "грубої сили" або словникових атак. Слабкі паролі залишаються однією з найпоширеніших та найлегших для експлуатації вразливостей. Незважаючи на рекомендації, багато користувачів продовжують використовувати прості та передбачувані паролі.

Відсутність або неналежне впровадження багатофакторної автентифікації, яка є ефективним способом захисту від несанкціонованого доступу, навіть у випадку компрометації пароля. Однак відсутність або неналежне впровадження MFA є значною вразливістю, яку активно експлуатують зловмисники. Ризики, пов'язані з відсутністю MFA, включають підвищену вразливість до фішингу, атак "грубої сили" та використання викрадених облікових даних. Слабкі реалізації MFA, такі як використання SMS-кодів, можуть бути перехоплені. Недостатнє охоплення MFA для всіх користувачів та систем також є проблемою. Незважаючи на доведену ефективність, MFA не завжди впроваджується належним чином або в достатньому обсязі. Організації можуть недооцінювати ризики або стикатися з труднощами при впровадженні MFA для всіх користувачів та систем.

Незахищене зберігання облікових даних є ще однією поширеною вразливістю. Зберігання паролів у вигляді відкритого тексту або використання слабких алгоритмів хешування для їх зберігання значно збільшує ризик компрометації. Зберігання API-ключів або токенів доступу в незахищених місцях, таких як код або файли конфігурації, також є поширеною помилкою. Небезпечне зберігання сесійних ідентифікаторів також може призвести до несанкціонованого доступу. Неналежне зберігання облікових даних значно збільшує ризик їх компрометації у випадку атаки на систему. Зловмисники, отримавши доступ до бази даних або файлів конфігурації, можуть легко отримати облікові дані, якщо вони не захищені належним чином.

Отже, для впровадження заходів ідентифікації користувачів до

інформаційної системи організації розглянемо основні підходи, які використовуються них.

1.2. Аналіз підходів до використання засобів ідентифікації користувачів інформаційної системи

Коли справа доходить до ідентифікації та безпеки, існує величезний океан різних варіантів автентифікації на вибір, які зможуть підвищити безпеку. Перш ніж прийняти або вибрати будь-який із методів автентифікації для співробітників або кінцевих користувачів організації, необхідно знати кілька ключових факторів, які допоможуть вибрати найбільш підходящий метод автентифікації.

Розглянемо деякі з найбільш розповсюджених та доступних методів автентифікації (рис.1.4).

Рис.1.4. Методи автентифікації користувачів інформаційної системи

1. Вхід на основі пароля. Найпоширеніша звичайна система автентифікації входу, яку користувачі використовують щодня під час користування онлайн-службою, — це вхід на основі пароля. Під час використання техніки автентифікації на основі пароля потрібно ввести комбінацію вашого імені користувача/номера мобільного телефону та пароля. Особа є авторизованою лише тоді, коли обидва ці елементи були перевірені. Однак, оскільки сучасні клієнти користуються кількома онлайн-сервісами (програмами та веб-сайтами), важко відстежувати всі їхні імена користувачів і паролі. У результаті цього кінцеві користувачі вчиняють неетичну поведінку, наприклад забувають паролі, використовують той самий пароль для кількох служб тощо. Кіберзлочинці проникають у цей момент і починають такі дії, як фішинг, витік даних тощо. Це фундаментальна причина, чому стандартна автентифікація на основі пароля втрачає прихильність і все більше організацій звертаються до розширених додаткових факторів автентифікації безпеки.

2. Багатофакторна автентифікація. Багатофакторна автентифікація (MFA) — це метод автентифікації, за якого особа повинна пройти кілька факторів, щоб отримати доступ до служби чи мережі. Це додатковий рівень безпеки на додаток до стандартного входу на основі пароля. Особи також повинні надіслати другий фактор у формі одноразового коду, який вони отримають телефоном або електронною поштою на додаток до свого імені користувача та пароля.

Ви можете швидко налаштувати кілька методів багатофакторної автентифікації (MFA), щоб забезпечити додатковий рівень безпеки для своїх ресурсів. OTP/TOTP через SMS, OTP/TOTP через електронну пошту, Push-сповіщення, апаратний маркер і мобільний автентифікатор — це приклади методів MFA (Google, Microsoft, Authy тощо). Ви можете вибрати будь-яку техніку MFA і застосувати її для організаційної безпеки відповідно до ваших потреб і вимог. Після традиційного входу на основі пароля багатофакторна автентифікація є найбільш надійним механізмом автентифікації. Для покращення безпеки традиційна автентифікація на основі пароля та методи багатофакторної автентифікації зазвичай використовуються одночасно.

3. Біометрична автентифікація. Індивідуальні фізичні атрибути, такі як відбитки пальців, долоні, сітківка ока, голос, обличчя та розпізнавання голосу, використовуються в біометричній автентифікації. Біометрична аутентифікація працює таким чином: спочатку фізичні характеристики людей зберігаються в базі даних. Щоразу, коли користувач хоче отримати доступ до будь-якого пристрою або фізично увійти в будь-яке приміщення (організація, школа, коледжі, робоче місце), фізичні особливості окремих осіб перевіряються на відповідність даним, що містяться в базі даних. Технологія біометричної автентифікації в основному використовується приватними організаціями, аеропортами та пунктами пропуску, де безпека є головним пріоритетом. Завдяки своїй здатності створювати високий рівень безпеки та зручний безперебійний потік, біометрія є однією з найбільш часто використовуваних технологій безпеки. Серед найпоширеніших методів біометричної аутентифікації:

1. Відбиток пальця. Автентифікація за відбитком пальця відповідає унікальному шаблону відбитка особи. У деяких вдосконалених системах автентифікації за відбитками пальців також визначається судинна структура пальця. Оскільки це одна з найбільш зручних і точних біометричних систем, автентифікація за відбитками пальців наразі є найпоширенішою біометричною технологією для звичайних клієнтів. Популярність біометрії може бути пов’язана з тим, що ви регулярно використовуєте свої мобільні телефони з відбитками пальців, а також компаніями чи установами, які використовують автентифікацію за відбитками пальців.

2. Сітківка та райдужна оболонка. сканери направляють яскраве світло в око та шукають характерні візерунки в барвистому кільці навколо зіниці ока в цій біометрії. Після цього сканований шаблон порівнюється з даними, записаними в базі даних. Коли людина носить окуляри або контактні лінзи, автентифікація на основі очей може бути неточною.

3. Обличчя. Під час автентифікації обличчя сканується кілька аспектів обличчя людини, коли вона намагається отримати доступ до певного ресурсу. Під

час порівняння обличчя під різними кутами або схожих осіб, наприклад членів сім'ї, результати розпізнавання обличь можуть бути суперечливими.

4. Розпізнавання голосу. Тон вашого голосу зберігається зі стандартизованим секретним кодом так само, як і вищезгаданий підхід. Перевірка відбувається, оскільки ви повинні говорити щоразу, коли хочете отримати доступ.

4. Аутентифікація на основі сертифіката.

Автентифікація на основі сертифіката ідентифікує людей, сервери, робочі станції та пристрої за допомогою електронної цифрової ідентифікації. У нашому повсякденному житті цифровий сертифікат функціонує подібно до водійських прав чи паспорта. Сертифікат складається з цифрової ідентифікації користувача, яка містить відкритий ключ і цифровий підпис центру сертифікації. Цей сертифікат підтверджує, що відкритий ключ і особа, яка видала сертифікат, є однією особою. Коли користувач намагається увійти на сервер, він повинен спочатку надати свій цифровий сертифікат. Сервер перевіряє ідентичність цифрового сертифіката та достовірність, підтверджуючи, що користувач має правильно пов'язаний закритий ключ із сертифікатом за допомогою криптографії.

5. Автентифікація на основі маркерів.

Автентифікація на основі маркерів дозволяє користувачам вводити свої облікові дані лише один раз і отримувати єдиний у своєму роді обмін зашифрованими рядками. Після цього вам не доведеться вводити свої облікові дані кожного разу, коли ви хочете увійти або отримати доступ. Цифровий маркер гарантує, що вам уже надано доступ. Більшість випадків використання, наприклад Restful API, доступ до яких здійснюється багатьма фреймворками та клієнтами, потребують автентифікації на основі маркерів.

6. Автентифікація єдиного входу (SSO). Єдиний вхід — це підмножина базової автентифікації на основі імені користувача та пароля. Перехід на автентифікацію SSO забезпечить розширену безпеку та численні функції для ваших кінцевих користувачів. Система єдиного входу, як вказано в назві, дозволяє окремим особам ввести своє ім'я користувача та пароль один раз і отримати доступ до всіх налаштованих програм. Завдяки цьому вам не потрібно запам'ятовувати

декілька паролів для різних програм, вам потрібно лише один раз увійти, і ви автоматично отримаєте доступ до всіх програм. Вигода від цього включатиме: оскільки користувачам потрібно запам’ятати лише один пароль, вони не забудуть його чи не запишуть його на будь-яких нотатках. Доступ до багатьох програм стане легшим, що підвищить ефективність і продуктивність. З боку адміністратора вони отримуватимуть менше дзвінків у службу підтримки щодо скидання пароля та проблем із входом [6-8].

7. Адаптивна автентифікація – це тип автентифікації, який адаптується до обставин». Адаптивна автентифікація, представляє більш просунутий вид 2FA/MFA автентифікації. Тут можна автентифікувати користувачів залежно від їхніх «IP-адреси, пристрою, місцезнаходження, пристрою та часу доступу». Якщо ввімкнено автентифікацію на основі IP-адреси та місцезнаходження, після введення імені користувача та пароля адаптивна автентифікація перевірить, чи збігається IP-адреса користувача з тим, який використовує адміністратор, і чи знаходиться він у місці, якому його було призначено. Якщо щось на збігається, йому буде відмовлено в доступі до ресурсів. Це один із найдосконаліших методів автентифікації, який використовують підприємства для забезпечення своєї безпеки.

Автентифікація API. Ссьогодні API став популярною моделлю, оскільки обробляє великі обсяги даних і є новим виміром у світі онлайн-безпеки. Методів аутентифікації API багато, найпопулярніші з них - HTTP Basic Auth, API keys, OAuth.

Базова автентифікація HTTP дозволяє підтвердити свою автентичність, агент користувача просто пропонує ім’я користувача та пароль. Оскільки воно підтримує сам заголовок HTTP, це рішення не потребує файлів cookie, ідентифікаторів сеансів або сторінок входу.

Паролі API — це унікальний ідентифікатор для запитів веб-служб, який ідентифікує їх джерело (або подібні типи запитів). Коли користувач намагається отримати дозволений доступ до системи вперше за допомогою реєстрації, створюється ключ. Після цього ключ API поєднується з секретним маркером і

надсилається з наступними запитами. Коли користувач намагається повторно увійти в систему, його унікальний ключ використовується для перевірки того, що це та сама особа, яка використовувала систему раніше.

OAuth — це популярна техніка автентифікації API, яка дозволяє як автентифікацію, так і авторизацію. OAuth дозволяє API автентифікувати та отримувати доступ до системи або ресурсу, за запитом, шляхом встановлення області.

У сучасному технологічному середовищі, яке швидко розвивається, безпека є найважливішим компонентом, щоб виділитися серед конкурентів і забезпечити бездоганний досвід для кінцевих споживачів.

Враховуючи вище сказане, можна сказати що для організацій доцільно використовувати комплексні системи ідентифікації та доступу. До таких систем відносяться системи Identity and Access Management (IAM). IAM гарантує, що правильні люди мають доступ до потрібної інформації у потрібний час. Кожна друга транзакція у світі відбувається онлайн, безпека стає не просто пріоритетом, а необхідністю [8].

IAM - це комплексна система, що охоплює багато процесів, які організація використовує для управління ідентифікацією користувачів та їх доступом до різних ресурсів організації.

Отже, надалі проведемо порівняння рішень IAM для проведення подальших досліджень.

1.3. Аналіз існуючих рішень ідентифікації користувачів інформаційної системи

Рішення для управління ідентифікацією та доступом (IAM) необхідні організаціям, які прагнуть захистити своє цифрове середовище та ефективно керувати ідентифікацією користувачів. Вони гарантують, що лише авторизовані користувачі мають доступ до конфіденційної інформації та програм [10].

Відповідно до проведеного дослідження щодо впливу атак на інформаційні

системи організації зрозуміло, що кращі інструменти управління ідентифікаційними даними могли б запобігти багатьом із цих інцидентів.

Завдяки рішенням для управління ідентифікацією та доступом організації можуть значно зменшити ймовірність того, що користувачі покладаються на слабкі паролі або паролі за замовчуванням, ефективно мінімізуючи пов'язані з цим ризики. Організації можуть інтегрувати свою IT-інфраструктуру з багатофакторною автентифікацією (MFA) і єдиним входом (SSO). Це посилить безпеку, що ускладнить зловмисникам зламати облікові записи.

Крім того, багато галузей мають суворі правила безпеки даних і конфіденційності (наприклад, GDPR, HIPAA та SOX). Рішення IAM спрощують відповідність цим стандартам, надаючи надійні журнали доступу та елементи керування.

Згідно з даними Gartner, найкращі рішення IAM включають керування життєвим циклом особистих даних, що включає створення та оновлення ідентифікаційних даних користувачів, автентифікацію, перевірку ідентифікаційних даних користувачів за допомогою облікових даних і авторизацію, а також визначення дозволів, наданих користувачам. У цих системах зазвичай використовується контроль доступу на основі ролей (RBAC), що дозволяє адміністраторам призначати права доступу на основі посадових функцій, таким чином мінімізуючи ризики, пов'язані з надмірними привілеями (рис.1.5).

Рішення IAM можна розгортати локально, у хмарі чи гібридному середовищі. Вони допомагають організаціям виконувати нормативні вимоги, запроваджуючи політику безпеки та надаючи журнали аудиту для дій користувачів. Компанії можуть захистити конфіденційні дані від несанкціонованого доступу, дозволяючи законним користувачам виконувати свої завдання, ефективно впроваджуючи IAM [10].

Попит на рішення IAM виріс для організацій за такої необхідності:

Покращена безпека. Рішення IAM значно підвищують рівень безпеки організації, гарантуючи, що лише авторизовані користувачі можуть отримати доступ до конфіденційних даних і ресурсів. Використовуючи надійні методи

автентифікації, такі як багатофакторна автентифікація та контроль доступу на основі ролей, IAM зменшує ризик несанкціонованого доступу та витоку даних.

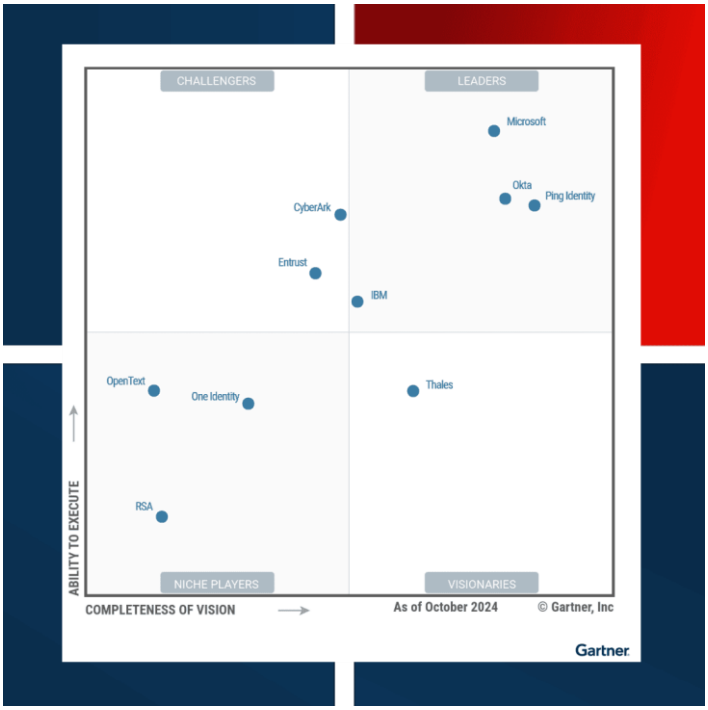


Рис.1.5. Кращі рішення IAM

Відповідність нормам. Багато галузей підпорядковуються суворим нормативним вимогам щодо конфіденційності та безпеки даних, зокрема Закону про перенесення та підзвітність медичного страхування (HIPAA), Загального регламенту захисту даних (GDPR) і Стандарту безпеки даних платіжних карток (PCI DSS). Рішення IAM допомагають організаціям дотримуватися цих правил, запроваджуючи контроль доступу та підтримуючи журнали аудиту.

Спрощене керування доступом. IAM автоматизує процеси ініціалізації та деініціалізації користувачів, а також запити та схвалення доступу. Ця автоматизація не тільки економить час IT-команд, але й мінімізує помилки, пов’язані з ручними процесами, що дозволяє організаціям працювати ефективніше.

Покращена взаємодія з користувачем і продуктивність. IAM покращує взаємодію з користувачем за допомогою таких функцій, як Single Sign-On (SSO), яка дозволяє користувачам отримувати доступ до кількох програм за допомогою одного набору облікових даних. Це не тільки спрощує процес входу, але й підвищує продуктивність, скорочуючи час, витрачений на керування кількома паролями.

Крім того, IAM забезпечує безпечний віддалений доступ, дозволяючи співробітникам ефективно працювати з різних місць без шкоди для безпеки.

Розглянемо деякі з провідних рішень IAM на основі рейтингів і оглядів Gartner Peer Insights [11] . Основні ключові функції та можливості рішень показано в таблиці 1.1.

Таблиця 1.1

Порівняльна таблиця рішень IAM

Критерій / Рішення	**SentinelOne Singularity Identity Security**	**Okta IAM (Identity Management)**	**IBM ISAM (та IBM Verify)**	**CyberArk Workforce Identity (раніше Idaptive)**
Опис	Захист інфраструктури ідентифікації (AD, Entra ID) від атак на основі ідентифікаційних даних, використання тактики обману.	Спрощення доступу користувачів та підвищення безпеки в різних програмах/службах, хмарна архітектура.	Керування ідентифікацією користувачів, контроль доступу до ресурсів, дотримання правил безпеки.	Забезпечення безпечного доступу для сучасної робочої сили до програм, кінцевих точок та інфраструктури.
Ключові функції	Запобігання атакам на AD/Entra ID. Виявлення та реагування в реальному часі (IDR). Зменшення поверхні атаки. Інтеграція з існуючими стеками (Okta, Azure AD, Ping).	Єдиний вхід (SSO). Багатофакторна автентифікація (MFA). Управління життєвим циклом. Керування доступом до API. Широкі можливості інтеграції	Автентифікація (MFA. Ідентифікаційна федерація (SAML, OAuth). Доступ з єдиною ідентифікацією (SSO). Керування веб-доступом.	Автоматизоване забезпечення користувачів. Керування життєвим циклом ідентифікації. Багаторівнева перевірка (MFA, контекстна). Вхід одним клацанням миші (SSO). Аналітика поведінки користувачів (AI)
Додаткові переваги / Вирішені проблеми	Глибока телеметрія для досліджень. Ефективне виявлення та	Покращена взаємодія з користувачем. Зменшення "втоми від паролів"	Безпечна співпраця з партнерами через федерацію. Зменшення навантаження на IT-	Динамічне налаштування прав доступу. Виявлення загроз в

	усунення загроз. Захист від розкриття конфіденційної інформації. Виявлення прихованих хмарних розгортань.		підтримку через самообслуговування.	реальному часі за допомогою ШІ.

Розкриємо суть кожного з рішень.

SentinelOne Singularity Identity Security

Singularity Identity від SentinelOne — це надійне рішення для кібербезпеки, призначене для захисту інфраструктур ідентифікації, особливо зосереджених на Active Directory (AD) і хмарних середовищах. Ця платформа призначена для захисту від атак на основі ідентифікаційних даних.

Singularity Identity пропонує проактивний, інтелектуальний захист у режимі реального часу для поверхні атак вашої інфраструктури ідентифікації. Організації можуть ефективно зменшити ризик ідентифікації в масштабах підприємства, використовуючи рішення як для Active Directory, так і для Entra ID. Цей підхід дозволяє не лише виявляти поточні атаки та реагувати на них, але також використовує тактику обману проти зловмисників у мережі.

Особливості.

SentinelOne проактивно *блокує загрози* на основі ідентифікаційної інформації, перш ніж вони зможуть використовувати Active Directory або Entra ID. Крім того, він визначає та зупиняє атаки на різних етапах, зупиняючи ескалацію та мінімізуючи потенційну шкоду.

Виявлення ідентифікації та реагування в режимі реального часу, зосереджені на захисті Active Directory, Entra ID та інших активів ідентифікації від різних загроз. Використовує передові методи машинного навчання та поведінкові методи для швидкого виявлення підозрілої активності.

Зменшення поверхні атаки ідентифікаційної інформації, зменшуючи вразливі точки в структурах ідентифікаційної інформації, ускладнюючи зловмисникам отримання неавторизованого доступу.

Okta IAM (керування ідентифікацією)

Okta є одним із провідних постачальників рішень IAM, який зосереджується на спрощенні доступу користувачів і підвищенні безпеки в різних програмах і службах. Платформа особливо відома своєю хмарною архітектурою, яка дозволяє організаціям ефективно керувати ідентифікацією та доступом.

Особливості.

Єдиний вхід надає користувачам плавний доступ до кількох програм за допомогою єдиного набору облікових даних, покращуючи взаємодію з користувачем і зменшуючи втому від пароля.

Багатофакторна автентифікація покращує безпеку, вимагаючи додаткових методів перевірки, крім паролів, таких як біометрія або одноразові коди.

Управління життєвим циклом. Інструмент автоматизує процеси реєстрації, виключення та керування ролями користувачів і правами доступу, гарантуючи, що користувачі мають відповідний доступ протягом усього періоду роботи.

Керування доступом до API за допомогою надійних механізмів автентифікації та авторизації, що дозволяє контролювати доступ до серверних служб.

Це рішення пропонує широкі можливості інтеграції з різними програмами та службами, що робить його придатним для різноманітних IT-середовищ, включаючи хмарні, локальні та гібридні налаштування.

Microsoft Entra

Microsoft Entra IAM розроблено для вирішення складних умов сучасного цифрового середовища. Він базується на можливостях Azure Active Directory (Azure AD) і пропонує кілька розширених функцій для підвищення безпеки, оптимізації взаємодії з користувачами та сприяння відповідності на різних платформах.

Особливості.

Керування привілейованою ідентифікацією (PIM) за допомогою своєчасного доступу, робочих процесів затвердження та моніторингу сеансів для зменшення ризиків, пов’язаних із підвищеними привілеями.

Управління ідентифікацією забезпечує видимість і контроль над ідентифікаторами користувачів і дозволами через рольовий контроль доступу (RBAC) і керування правами. Це гарантує, що потрібні люди завжди матимуть належний доступ.

Уніфікований вхід спрощує автентифікацію користувачів, увімкнувши SSO, що дозволяє користувачам отримувати доступ до кількох програм за допомогою одного набору облікових даних.

Дворівнева безпека, для подальшого посилення безпеки Entra підтримує MFA, що вимагає додаткових методів перевірки, таких як біометрія або одноразові паролі.

IBM ISAM

IBM пропонує ряд рішень для керування ідентифікацією та доступом, головним чином через IBM Security Identity and Access Manager (ISAM) і IBM Verify. Ці рішення розроблені, щоб допомогти організаціям керувати ідентифікацією користувачів, контролювати доступ до ресурсів і дотримуватися правил безпеки.

Особливості.

Автентифікація посилює безпеку, вимагаючи від користувачів надавати кілька форм автентифікації під час входу.

ISAM підтримує федеративну ідентифікацію від зовнішніх постачальників ідентифікаційної інформації за допомогою таких протоколів, як SAML і OAuth, сприяючи безпечній співпраці з партнерами.

Доступ з єдиною ідентифікацією - користувачі можуть отримати доступ до кількох програм за допомогою одного набору облікових даних, покращуючи взаємодію з користувачем і зменшуючи втому від пароля.

Керування веб-доступом надає централізований контроль над доступом користувачів до веб-додатків і забезпечує відповідність політикам доступу.

Самообслуговування користувача - користувачі можуть самостійно виконувати такі завдання, як скидання пароля, зменшуючи навантаження на IT-підтримку.

CyberArk Identity

CyberArk Identity (раніше Idaptive) — це набір рішень для керування ідентифікацією та доступом, створених для забезпечення безпечного доступу для сучасної робочої сили. Він забезпечує безпечний безперешкодний доступ до програм, кінцевих точок і критичної інфраструктури з ключовими рішеннями, зосередженими на управлінні доступом, керуванні ідентифікацією та привілейованим доступом.

Особливості.

Рішення автоматизує процеси реєстрації та виключення користувачів, забезпечуючи динамічне налаштування прав доступу відповідно до зміни ролей в організації.

Керування життєвим циклом ідентифікації. Ця функція спрощує керування ідентифікаторами користувачів протягом усього життєвого циклу, від початкової реєстрації до остаточного відходу, забезпечуючи відповідність і зменшуючи адміністративні витрати.

Багаторівнева перевірка підвищує безпеку, вимагаючи кількох форм перевірки, які можна адаптувати на основі контекстних факторів, таких як місцезнаходження користувача та тип пристрою.

Функція SSO CyberArk дозволяє користувачам отримувати доступ до кількох програм за допомогою одного набору облікових даних, зменшуючи втому від пароля та покращуючи взаємодію з користувачем.

CyberArk використовує аналітику на основі ШІ для моніторингу поведінки користувачів, допомагаючи виявляти потенційні загрози безпеці та реагувати на них у режимі реального часу.

Отже для подальшого дослідження обираємо CyberArk Identity, яке дозволяє керувати життєвим циклом ідентифікації та надає послуги з використання різних засобів ідентифікації користувачів інформаційної системи організації.

2 ЗАСОБИ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ІНФОРМАЦІЙНОЇ СИСТЕМИ

2.1. Архітектура платформи CyberArk Identity

CyberArk Identity — це набір рішень SaaS, розроблений для спрощення ідентифікації та керування доступом на підприємствах. CyberArk Identity об'єднує рішення для доступу до персоналу та керування ідентифікацією в одній пропозиції. Можливості Workforce Access включають єдиний вхід, багатофакторну автентифікацію, безпеку сеансу та керування обліковими даними. Можливості керування ідентифікацією включають керування життєвим циклом, оркестровку ідентифікації та керування ідентифікацією. За допомогою CyberArk Identity організації можуть забезпечити доступ працівників до програм, кінцевих точок та інфраструктури та захистити себе від основної причини витоку даних – скомпрометованих облікових даних.

CyberArk Identity складається з таких служб, веб-порталів для адміністраторів і користувачів, а також мобільних програм, які користувачі можуть інсталювати на своїх пристроях iOS і Android [12].

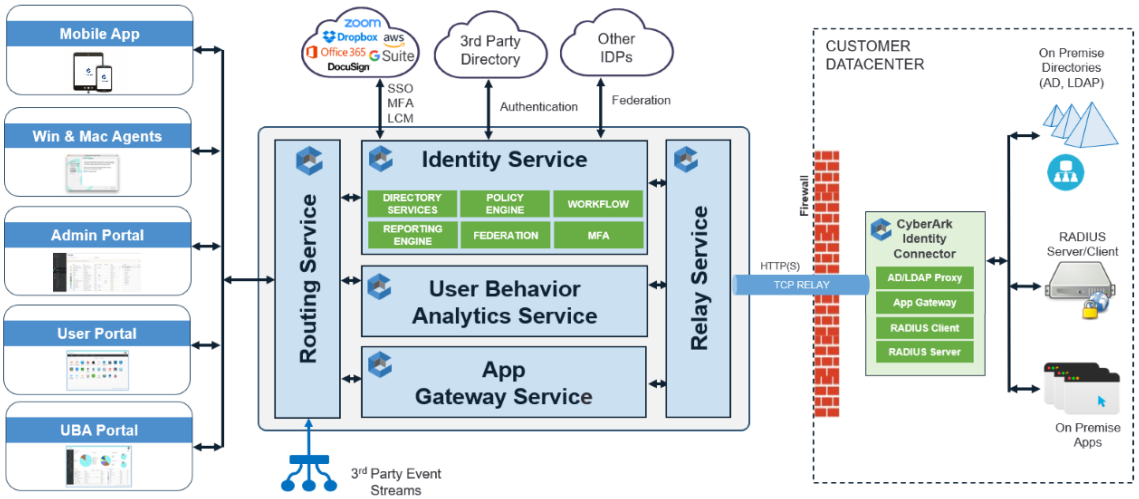


Рис.2.1. Архітектура платформи CyberArk Identity

До основних сервісів, які надає CyberArk Identity відноситься:

CyberArk Identity Single Sign-On (SSO) – надає працівникам зручний доступ одним клацанням миші до всіх своїх корпоративні програми, використовуючи єдиний набір облікових даних. Рішення допомагає зменшити розповсюдження пароля та покращити взаємодію з користувачами, що допомагає уникнути ризикованих обхідних шляхів, як-от використання звичайних облікових даних або запис паролів на папері або в електронних таблицях. Рішення також централізує, уніфікує та спрощує адміністрування доступу, зменшення взаємодії зі службою підтримки та операційних витрат [13].

Адаптивна багатофакторна автентифікація CyberArk Identity (MFA) – допомагає компаніям уникати даних втрата та інші ризики, спричинені зламаними або викраденими обліковими даними. Рішення підтримує різноманітні механізми автентифікації, включаючи безпарольні фактори, і захищає ряд ідентифікаційних даних підприємства та ресурси, такі як програми, інфраструктура та кінцеві точки. На відміну від традиційних рішень MFA, CyberArk Identity Adaptive MFA використовує аналітику поведінки на основі ШІ та контекстну інформацію, щоб визначити, які фактори автентифікації для застосування до конкретного користувача в конкретній ситуації, покращуючи задоволеність кінцевого користувача продуктивність [13].

CyberArk Identity Lifecycle Management (LCM) – допомагає адміністраторам ефективно впроваджувати нових користувачів та керувати їхніми привілеями доступу протягом усього циклу роботи. Рішення містить інструменти самообслуговування для користувачів і менеджерів, які затверджують, а також командам безпеки відстежувати активність доступу, розслідувати інциденти та підтримувати аудит відповідності. Інтеграція з провідними системами управління персоналом, рішеннями для управління ідентифікацією та адмініструванням, а також службами каталогів спрощує надання нових користувачів і усуває процеси, схильні до помилок.

CyberArk Identity App Gateway – допомагає користувачам отримати безпечний доступ до традиційних програм, розміщених у корпоративних центрах обробки

даних, використовуючи ті самі облікові дані та методи автентифікації, які вони використовують для доступу до хмарних програм.

CyberArk Identity Directory Services – дає змогу організаціям централізовано керувати корпоративними IT-каталогами в масштабі. Рішення інтегрується з низкою популярних локальних і хмарних служб каталогів, включаючи Microsoft Active Directory, Azure Active Directory і каталоги LDAP. Розширювана схема дозволяє легко підтримувати інформацію, пов'язану з користувачами, комп'ютерами, кінцевими точками, мобільними та серверними об'єктами та іншими елементами, використовуючи уніфіковане сховище даних і загальні засоби адміністрування

CyberArk Identity User Behavior Analytics – використовує ШІ та машинне навчання для збору, аналізу та візуалізації поведінки користувачів і даних про загрози в режимі реального часу. Рішення містить інтерактивні інформаційні панелі для допомоги адміністратори легко оцінюють ризики, інструменти звітування, які допомагають адміністраторам розслідувати інциденти безпеки та підтримують аудити, а також сповіщення в реальному часі для сповіщення адміністраторів про підозрілу активність. Він також надає веб-куки для передачі сповіщень стороннім інструментам, таким як ServiceNow.

CyberArk Identity інтегрується з AWS SSO як постачальник ідентифікаційних даних для AWS Control Tower (рис.2.2), автоматично налаштовуючи користувачів і групи для забезпечення спрощеного безпечного доступу користувачів до авторизованих облікових записів і ресурсів AWS.

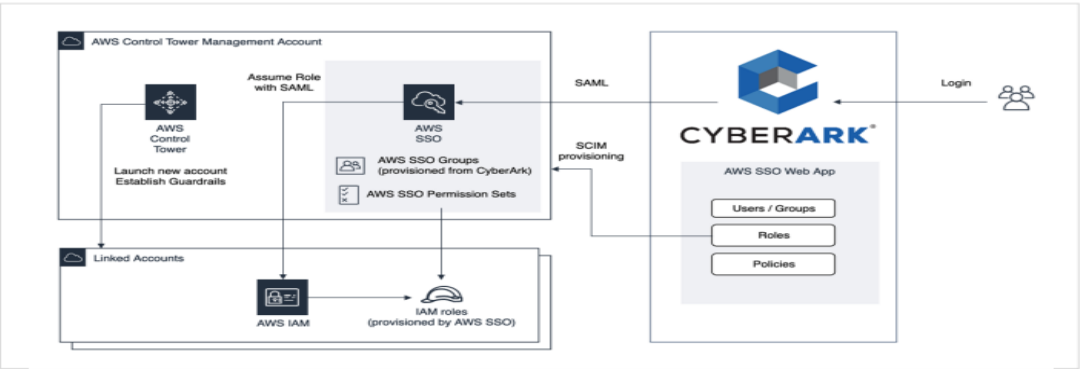


Рис.2.2. Інтеграція CyberArk Identity з AWS SSO

CyberArk Identity надає ролі та політики, які дозволяють детально контролювати, що можуть робити різні користувачі та де потрібна багатофакторна автентифікація (MFA). Залежно від послуг, якими надаються користувачеві, політики дозволяють контролювати роботу та поведінку в наведених нижче категоріях.

Таблиця 2.1.

Категорії політик та їх опис

Категорія	**Опис**
Політика мобільних пристроїв	Керування пристроєм та реєстрація. API політики надає доступ до можливостей, які є специфічними для певних виробників, наприклад, iOS і Samsung.
Політика безпеки облікового запису	Керуйте безпекою облікового запису, включаючи скидання пароля та вимоги до пароля, такі як довжина та складність. Механізм політики також підтримує встановлення та застосування багатофакторної автентифікації, тобто вимагання від користувачів додаткової автентифікації, наприклад коду, отриманого з текстового повідомлення чи електронної пошти.
Політика програми	Укажіть, чи дозволено користувачам додавати програми на свої пристрої.
Аутентифікація	Політики також дозволяють визначати складні правила автентифікації та профілі для реалізації багатофакторної автентифікації за допомогою SMS, голосового дзвінка, таємного запитання, електронної пошти, одноразового коду доступу одним дотиком або автоматичного push-повідомлення на мобільні пристрої.

Робочий процес, необхідний для підготовки та налаштування служб платформи показано на рис 2.3.

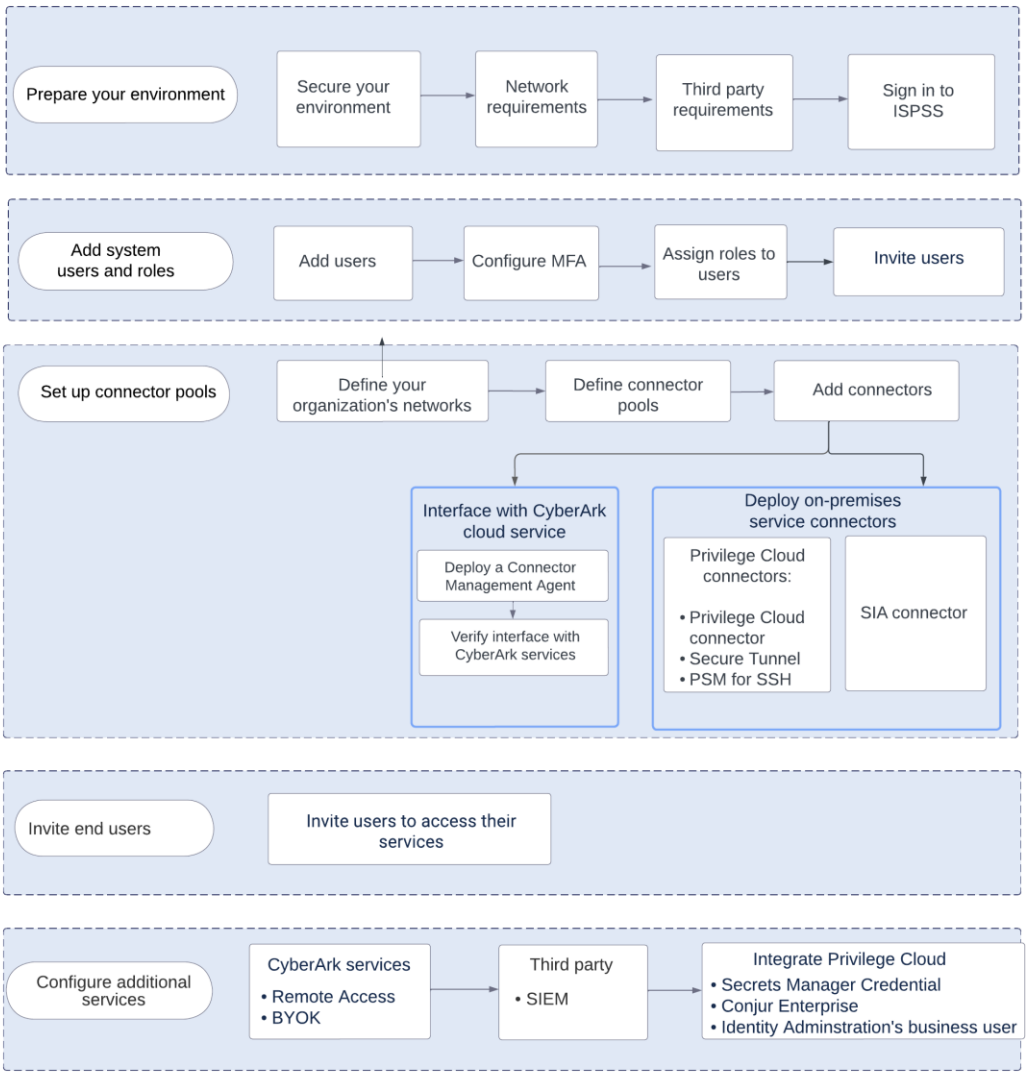


Рис.2.3. Проце розгортання ISPSS

Отже, дана платформа є гарним інструментом, який до зволяє надавати користувачам інформаційної системи організації відповідні послугі щодо ідентифікаії. Тож надалі розглянемо види користувачів та їх ролі в інформаційній системі організації.

2.2. Типи користувачів та їх ролі

В ISPSS існує два основних типи користувачів: інтерактивні користувачі та користувачі служб (табл.2.2) [14].

Таблиця 2.2.

Типи користувачів ISPSS

Тип користувача	**Опис**
Інтерактивні користувачі	Будь-який користувач, який входить до cyberark для взаємодії з а обслуговування портал (наприклад, портал користувача).
Користувачі служб	Користувач сервісу, призначений для завдань API та автоматизації. Цей користувач має мінімальні права доступу, йому не призначено політики MFA, і він не може отримати доступ до адміністрування ідентифікаційної інформації .

Інтерактивні користувачі — це користувачі для доступу кінцевих користувачів до порталу користувача та будь-якої підтримуваної служби CyberArk.

Інтерактивні користувачі визначаються вручну або імпортуються з таких джерел:

1. Зовнішній каталог на основі вашого рішення автентифікації:

– Рішення локальної автентифікації , наприклад Microsoft Active Directory, LDAP або RADIUS.

– Хмарна автентифікація, наприклад Microsoft Entra ID або Google Workspace.

2. Зовнішній постачальник ідентифікаційної інформації (IdP) використовує маркер SAML для надання доступу до ресурсів, якими ви хочете поділитися.

Користувачі служб - використовуються для неінтерактивного API і поділяються на:

1. Користувачі служби підтримки клієнтів:

Будь-який користувач, якому потрібно запускати API та завдання автоматизації, повинен використовувати користувача служби.

2. Внутрішні користувачі служби:

Внутрішні користувачі служб, вбудовані в ISPSS для внутрішніх завдань. Ці користувачі можуть відображатися у звітах користувачів і аудитах, створених у різних службах ISPSS.

Користувачі можуть отримати доступ до певної служби CyberArk , лише якщо їм призначено роль із правами доступу до цієї служби. Для кожної служби доступні вбудовані ролі для визначення рівнів доступу для кожного користувача в цій службі. Ролі можна призначати групі користувачів або одному користувачеві.

Існує чотири основних типи контролю доступу. Організації зазвичай обирають метод, який є найбільш доцільним на основі їхніх унікальних вимог до безпеки та відповідності. Чотири моделі контролю доступу:

Дискреційне керування доступом (DAC): у цьому методі власник або адміністратор захищеної системи, даних або ресурсу встановлює правила для того, кому дозволено доступ.

Обов'язковий контроль доступу (MAC): у цій недискреційній моделі людям надається доступ на основі дозволу інформації. Центральний орган регулює права доступу на основі різних рівнів безпеки. Ця модель поширена в урядових і військових середовищах.

Контроль доступу на основі ролей (RBAC): RBAC надає доступ на основі визначених бізнес-функцій, а не ідентифікаційних даних окремого користувача. Мета полягає в тому, щоб надати користувачам доступ лише до тих даних, які вважаються необхідними для виконання їхніх ролей в організації. Цей широко використовуваний метод базується на складній комбінації призначень ролей, повноважень і дозволів.

Контроль доступу на основі атрибутів (ABAC): у цьому динамічному методі доступ ґрунтується на наборі атрибутів і умов навколишнього середовища, таких як час доби та місцезнаходження, призначених користувачам і ресурсам.

CyberArk Identity надає ролі на основі моделі RBAC, яка працює, призначаючи користувачам ролі, які, у свою чергу, мають пов'язані з ними дозволи [18].

Ці дозволи визначають, які дії може виконувати користувач і до яких ресурсів він може отримати доступ. Такий підхід спрощує процес керування правами користувачів, оскільки більше не потрібно призначати дозволи на індивідуальній основі.

Натомість керування доступом стає питанням призначення відповідної ролі обліковому запису користувача. Ця структура не тільки спрощує процес налаштування, але й підвищує безпеку, мінімізуючи ризик неналежного надання доступу.

Приклади RBAC

Щоб краще зрозуміти RBAC, уявіть собі таблицю дозволів, що відповідають різним ролям у програмі. Наприклад (рис 2.4):

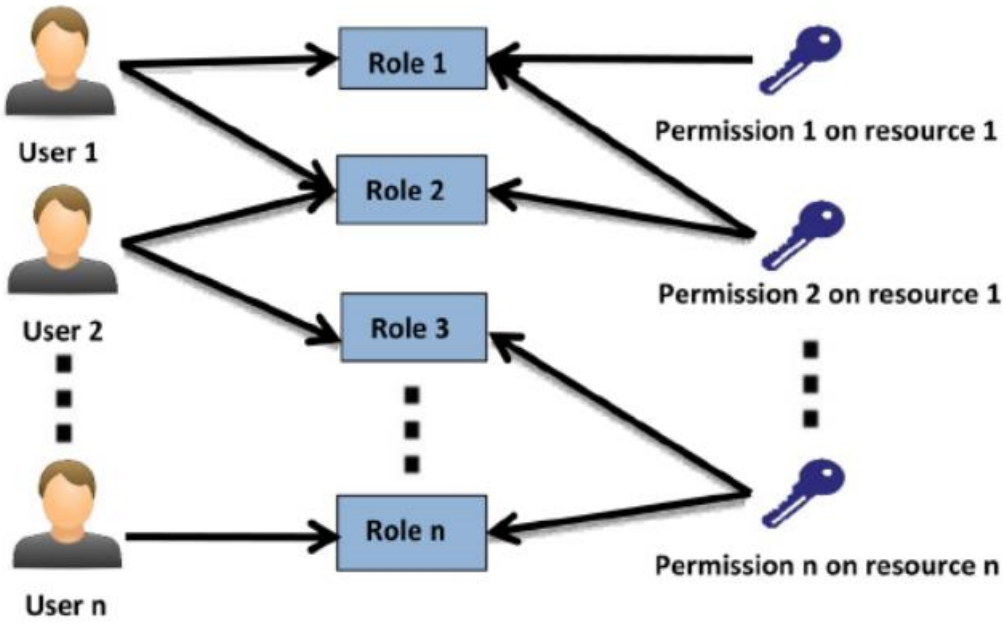


Рис.2.4. Принцип ролевої моделі RBAC

Клієнт : може переглядати товари та робити покупки.

Менеджер з продажу : може переглядати та редагувати списки продуктів, отримувати доступ до звітів про продажі та керувати замовленнями клієнтів.

Системний адміністратор: має повний доступ, включаючи керування користувачами, налаштування системи та доступ до всіх даних.

CyberArk Identity надає користувачам ролі як частину системи Privilege Cloud з різними типами ліцензій користувача і дозволяє розширити свій початковий пакет системи, включивши нові типи ліцензій користувача.

Основні параметри ліцензії користувача:

– Привілейований базовий користувач.
– Привілейований стандартний користувач Lite.
– Привілейований стандартний користувач.
– Привілейований зовнішній користувач.

Для додавання користувачів до CyberArk Identity можна використовувати декілька способів щоб розгорнути Identity Connector:

Додавання користувачів із служби каталогів.

Додавання користувачів CyberArk Cloud Directory.

Додавання користувачів сервісу.

Замовити пошук служби каталогів.

CyberArk Identity дозволяє налаштувати MFA для всіх користувачів або користувачів із певними ролями.

Можна налаштувати, щоб користувачі завжди проходили автентифікацію, незалежно від факторів підключення чи умов. Наприклад, якщо ви створюєте профіль автентифікації лише з вибраним механізмом пароля та призначаєте його параметру Профіль за замовчуванням, тоді всім користувачам (незалежно від IP-адреси комп'ютера для входу та ідентифікаційних файлів cookie браузера) буде запропоновано ввести паролі.

2.3. Протоколи автентифікації CyberArk Identity

Для користувачів CyberArk Identityнадає послуги автентифікації за різнимим протоколами, такими як RADIUS та LDAP. Дослідимо сутність з кожного протоколу [19].

Служба доступу до віддаленої автентифікації (RADIUS) — це мережевий протокол, який авторизує та автентифікує користувачів, які отримують доступ до

віддаленої мережі. Протокол — це набір правил, які контролюють, як щось обмінюється даними або працює.

RADIUS використовується для встановлення з'єднань між комп'ютерами та забезпечує автентифікацію, авторизацію та облік. RADIUS є важливим інструментом для керування доступом до мережі, оскільки він може запобігти проникненню неавторизованих користувачів і зловмисників у вашу мережу.

Протокол RADIUS використовує клієнт RADIUS або сервер доступу до мережі (NAS) і сервер RADIUS. Він виконує деякі з тих самих функцій, що й полегшений протокол доступу до каталогу (LDAP) , і надає служби локальної автентифікації, зберігаючи активний каталог облікових даних користувача. Його функції безпеки ставлять його на один рівень із протоколом керування передачею (TCP) . RADIUS працює на портах 1812 і 1813.

Походження протоколу RADIUS

RADIUS був розроблений компанією Livingston Enterprises, Inc. у 1991 році та перетворився на стандарт для Інженерної робочої групи Інтернету (IETF). RADIUS вперше використовувався для підключення університетів штату Мічиган. Національний науковий фонд (NSF) надав грант некомерційному інтернет-провайдеру Merit Network, і вони уклали контракт з Livingston Enterprises на розробку протоколу, який у підсумку став RADIUS.

Основні функції протоколу RADIUS

RADIUS виконує три основні функції: аутентифікація, авторизація та облік [19].

Автентифікація: RADIUS перевіряє автентифікацію пристроїв або користувачів, перш ніж дозволити їм отримати доступ до мережі.

Авторизація : RADIUS авторизує пристрої або користувачів, дозволяючи їм використовувати певні служби в мережі.

Облік: RADIUS враховує кількість використаних ресурсів, таких як пакети, байти та витрачений час, під час сеансу.

Робота сервера RADIUS базується на протоколі дейтаграм користувача (UDP) , і зазвичай це програма-демон, яка працює на комп'ютері Windows або

UNIX. Демон — це програма, яка працює у фоновому режимі. Сервер RADIUS збирає ідентифікаційну інформацію про всі облікові дані своїх користувачів. Сервер чекає, доки не отримає запит від клієнта або NAS, які можуть бути пристроями чи системами, такими як бездротові точки доступу або віртуальні приватні мережі (VPN)) рис.2.5.

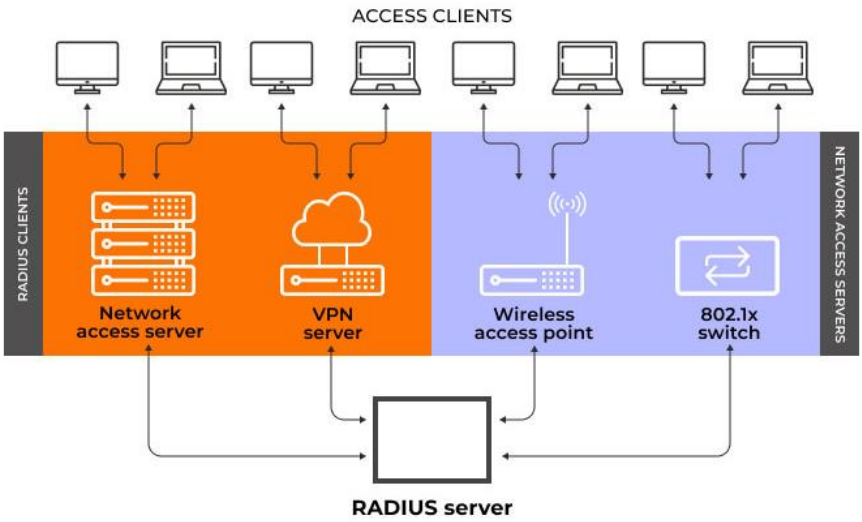


Рис.2.5. Архітектура протоколу RADIUS

Як тільки сервер RADIUS отримує цю інформацію, він надсилає відповідь клієнту. Таким чином RADIUS-сервери отримують запити на підключення від користувачів, автентифікують кожного користувача, а потім повертають необхідні деталі конфігурації, щоб клієнт міг надати користувачеві послугу. Процес ,як відбувається підключення в CyberArk Identity показано на рис.2.6 [20].

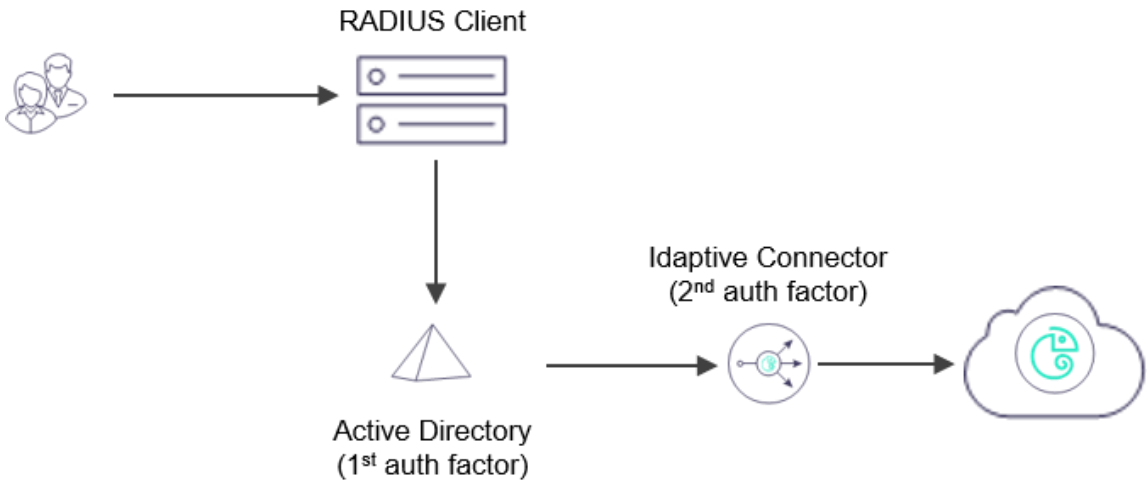


Рис.2.6. Процес автентифікації через RADIUS в CyberArk Identity

Сервер RADIUS надає користувачам переваги, включаючи масштабоване рішення, яке можна легко модифікувати для різних систем безпеки, одночасно розділяючи процеси зв’язку та безпеки.

Для автентифікації мережі RADIUS використовує модель клієнт/сервер. Повідомлення, що надсилаються туди й назад, дають змогу адміністраторам перевірити, хто має доступ до з’єднання, використовуючи базу даних, що містить схвалені облікові дані користувача.

Користувач надсилає запит на сервер доступу до мережі (NAS).

Першим кроком у підключенні за допомогою сервера RADIUS є надсилання користувачем запиту до NAS. Це можна зробити за допомогою ряду мережевих ресурсів, наприклад, стільникових телефонів або персональних комп’ютерів. Програма, призначена для надсилання запитів на вхід, називається запитувачем, передає облікові дані користувача до NAS. Це може включати мережеву адресу користувача, ім’я користувача та пароль.

NAS надсилає запит на доступ до сервера RADIUS.

Наступний крок у процесі підключення відбувається, коли NAS надсилає повідомлення із запитом на доступ до сервера RADIUS. Спочатку NAS отримує дані користувача, а потім надсилає їх через запит. Сервер перевіряє, чи запит на доступ надходить із законного джерела, порівнюючи його з інформацією, що зберігається в його базі даних.

Сервер RADIUS відповідає на запит доступу.

Коли сервер RADIUS отримує повідомлення, він може відповісти трьома різними способами: прийняти доступ, відхилити його або оскаржити його. Коли запит на доступ прийнято, доступ надається. Якщо запит відхилено, доступ не надається, а в разі виклику RADIUS-сервер запитує додаткову інформацію, перш ніж дозволити доступ.

Коли доступ приймається, це робиться відповідно до атрибутів авторизації, які є умовами, які визначають, як користувач матиме доступ. Деякі з них можуть включати тривалість підключення користувача, тип протоколу, який буде

використовуватися, або адресу Інтернет-протоколу (IP), яку користувач матиме під час сеансу.

Коли користувачі намагаються ввійти в CyberArk Identity і вибирають зовнішній RADIUS-сервер як механізм багатофакторної автентифікації (MFA), система надсилає облікові дані користувача (ім'я користувача та пароль) на з'єднувач, який перевіряє їх на налаштований RADIUS-сервер і повертає результат цієї перевірки в CyberArk Identity . На рис.2.7. показано робочий процес такого підключення [20].

Рис.2.7. Налаштування CyberArk Identity для RADIUS [20]

Облік RADIUS використовується окремо від процесів авторизації та автентифікації та дозволяє надсилати дані після завершення сеансу. Ці дані описують такі елементи, як надіслані пакети даних, тривалість сеансу та кількість надісланих даних.

Дані корисні для виставлення рахунків і моніторингу, оскільки вони враховують усі ресурси, використані під час активного сеансу. Наприклад, якщо користувачеві виставляється рахунок відповідно до обсягу даних, які він використовує, функція обліку надасть підрахунок. Крім того, якщо адміністратор хоче знати, яку інформацію було передано, він може використовувати функцію обліку RADIUS, щоб відстежувати діяльність, що виконується під час сеансу.

Розглянемо інший протокол, який застосовується в CyberArk Identity для автентифікації користувачів – протокол LDAP [21].

Полегшений протокол доступу до каталогу (LDAP) — це відкритий міжплатформний програмний протокол, який використовується для автентифікації та зв’язку в службах каталогів. LDAP забезпечує мову, яку програми використовують для спілкування одна з одною в службах каталогів, які зберігають облікові записи комп’ютерів, користувачів і паролі та обмінюються ними з іншими об’єктами в мережі. Це дозволяє додаткам і користувачам знаходити та перевіряти потрібну інформацію з усієї організації.

LDAP має широкий спектр використання, але найпопулярнішим є як центральний центр для організацій для керування автентифікацією. Це дуже ефективно, оскільки допомагає організаціям зберігати, керувати та отримувати доступ до імен користувачів і паролів у своїх мережах і програмах. Якщо організації використовують правильні плагіни, LDAP дає їм змогу зберігати та перевіряти облікові дані кожного разу, коли користувач намагається отримати доступ до програм, каталогів і систем.

Облікові дані LDAP включають не лише стандартні комбінації імені користувача та пароля. Протокол також можна використовувати для керування іншими організаційними атрибутами, такими як зберігання адрес, структурних даних і номерів телефонів, що робить його вкрай важливим для керування та захисту ідентифікаційних даних користувачів. LDAP також з’єднує користувачів з інформацією про пристрої, під’єднані до мережі, як-от файли, принтери та спільні ресурси.

Завдяки своїй здатності взаємодіяти зі службами каталогів, такими як Microsoft Active Directory (AD), LDAP є важливим інструментом для бізнесу. Протокол використовується для зв’язку з AD і з’єднує клієнтів — комп’ютери, які підключаються до віддалених комп’ютерів або серверів і використовують їх ресурси — до необхідної інформації в службах каталогів.

По суті, LDAP забезпечує ефективну спільну мову, яка спрощує процес надання відповідей на запити клієнтів. При безпечному використанні він дозволяє організаціям створювати ефективні бази даних і керувати ними, а також надає співробітникам інструменти, необхідні для ефективної та продуктивної роботи.

LDAP — це мова, яка дозволяє серверам спілкуватися з AD та іншими службами каталогів. Це дозволяє повідомленням, таким як запити клієнта, відповіді сервера та форматування даних, передавати між серверами та клієнтськими програмами.

Цей процес працює за допомогою LDAP (рис.2.8), прив'язуючи користувачів до сервера. Коли клієнт надсилає запит на певну інформацію, таку як облікові дані користувача, сервер LDAP обробляє його, використовуючи свою внутрішню мову, а потім зв'язується зі службами каталогів перед надсиланням відповіді. Коли клієнт отримує відповідь, LDAP від'єднує клієнта від сервера, і клієнт обробляє дані.

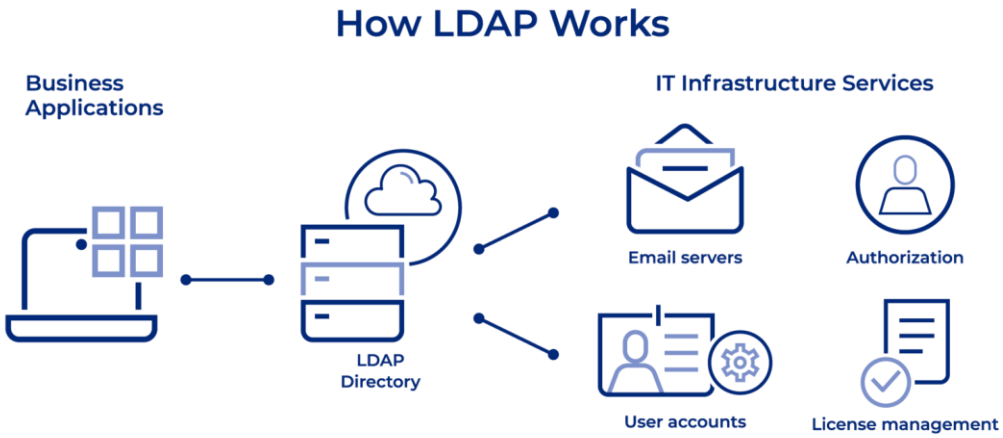


Рис.2.8. Процес роботи протоколу LDAP

Інше використання LDAP включає в себе System Security Services Daemon (SSSD), яке є програмним забезпеченням, спочатку створеним для операційних систем Linux і надає спрощений доступ до різних постачальників віддаленої ідентифікації та автентифікації. SSSD можна налаштувати для використання власних доменів LDAP, наприклад постачальника ідентифікаційної інформації LDAP з автентифікацією LDAP або постачальника ідентифікаційної інформації LDAP з автентифікацією Kerberos.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ВПРОВАДЖЕННЯ ЗАСОБІВ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ІНФОРМАЦІЙНОЇ СИСТЕМИ

3.1 Варіант впровадження засобів ідентифікації користувачів інформаційної системи на базі CyberArk Identity

Для виконання данного розділу в роботі буде використовуватися демо-версія хмарного CyberArk Identity для налаштування MFA та SSO.

Після отримання демо-версії ми переходимо інформаційної панелі рішення,яку показано на рис.3.1.

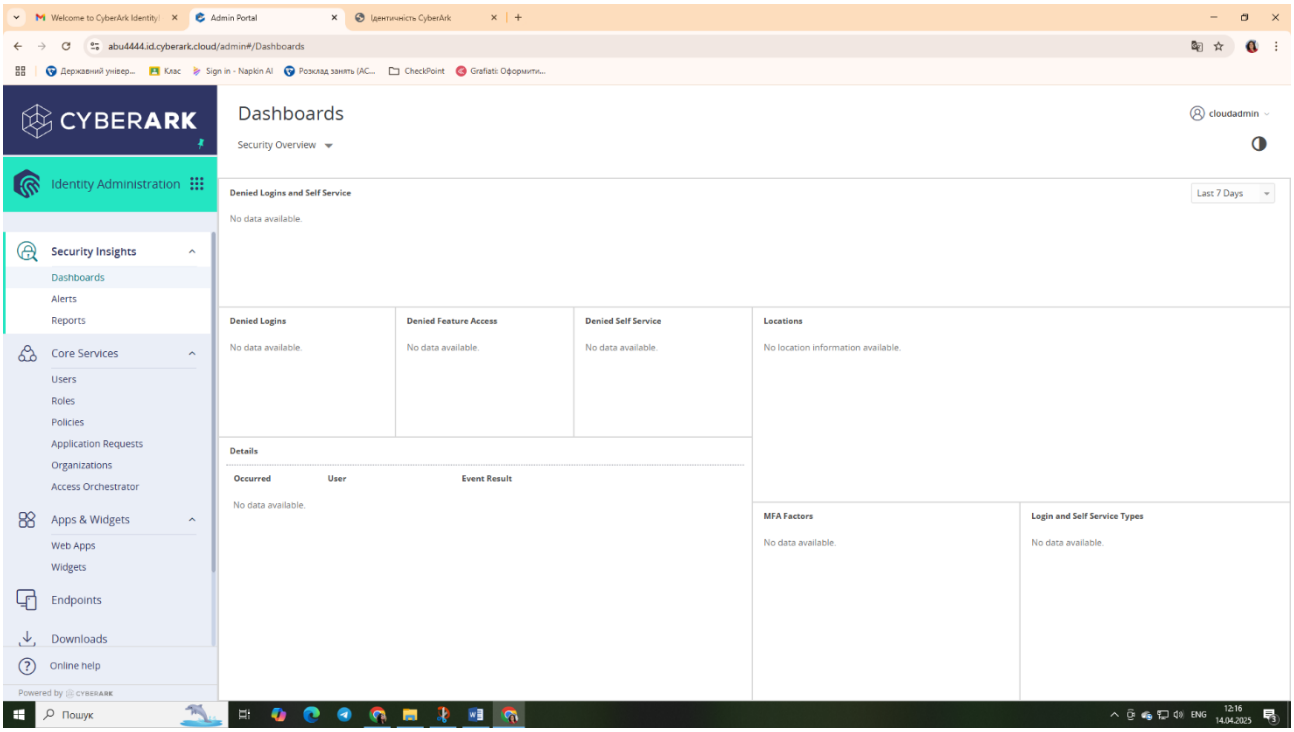


Рис.3.1. Інформаційна панель CyberArk Identity

CyberArk Identity дозволяє дуже легко зіставляти групи безпеки AD з ролями для інтеграції SSO, багатофакторної автентифікації (MFA) і політик безпеки кінцевих точок. Ця функція дозволяє керувати даними AD у хмарі без дублювання.

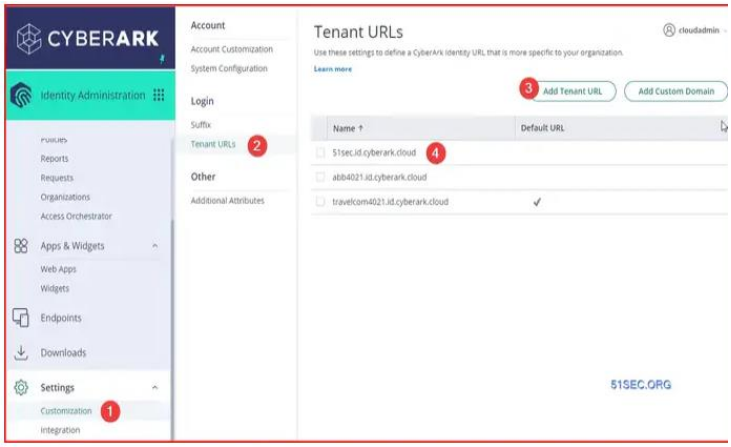
1. Налаштуємо власну URL-адресу клієнта:

Портал адміністратора ідентифікації – Параметри – Налаштування – URL-адреси орендарів – Додати URL-адресу орендарів

https://51sec.id.cyberark.cloud

https://travelcom4021.id.cyberark.cloud/

https://abb4021.id.cyberark.cloud/



3.2. Налаштування URL-адресу клієнта

Змінивши суфікс користувача можна увійти за допомогою admin@51sec цього облікового запису в Identity Cloud.

2. Створіть/оновіть Installeruser

Обліковий запис служби InstallerUser — це вбудований обліковий запис, який існує в клієнті Identity Security Platform Shared Services (ISPSS). Цей обліковий запис не вбудовано в орендаря безкоштовної пробної версії. Для внутрішніх змін із клієнтом ISPSS потрібне використання вбудованого облікового запису InstallerUser.

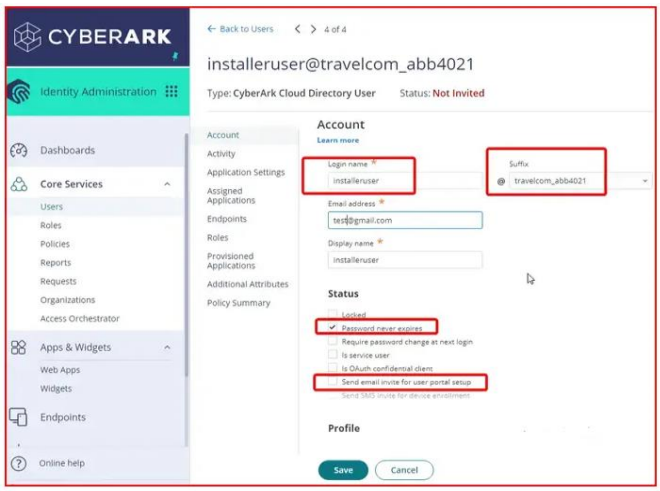


Рис.3.3. Створення Installeruser

Додаємо обліковий запис InstallerUser до ролі системного адміністратора.

3. Встанлюємо Identity Connector

4. Зареєструємо CyberArk Identity Connector на клієнті Identity (рис.3.4).

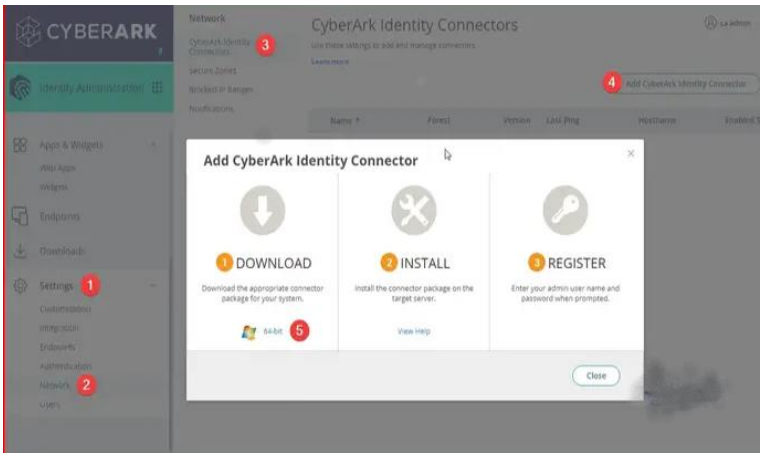


Рис.3.4. Реєстрація CyberArk Identity Connector на клієнті Identity

Після встановлення CyberArk Identity Connector можемо підключати користувачів до системи ідентифікації.

1. Створюємо одного користувача

— Виберіть суфікс

- вручну встановити пароль / автоматично згенерувати

- надсилати запрошення чи ні

2. Використання масового імпорту користувачів

- завантаження шаблону

3. Перевірте Резюме політики користувача

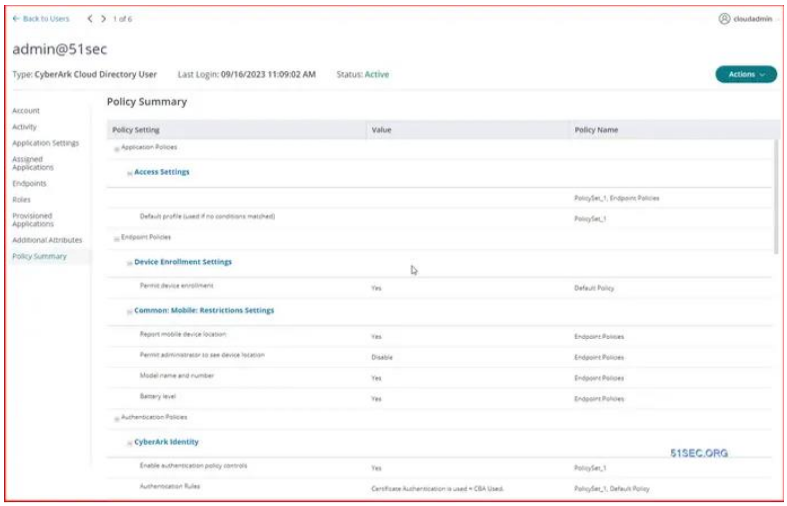


Рис.3.5. Реєстрація користувача

Налаштовуємо ідентифікаційні ролі (схожі на групові).

Лише глобальні адміністратори можуть створювати політики та керувати ними в CyberArk Identity.

Ролі ідентифікації подібні до групи безпеки AD. Перегляд ролей CyberArk Identity за замовчуванням.

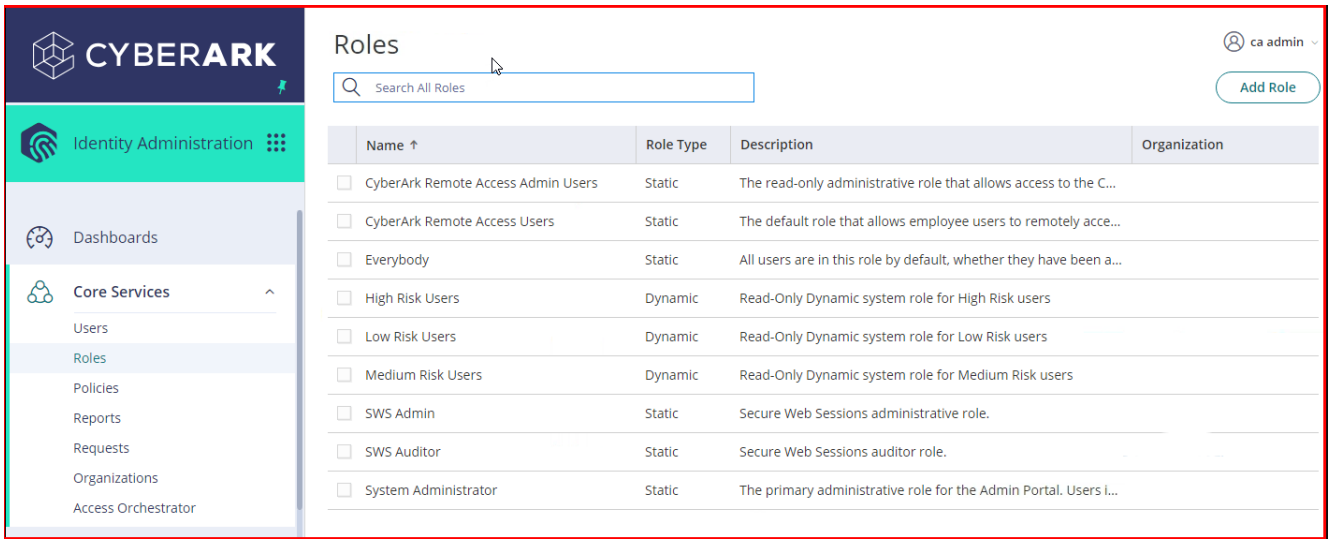


Рис.3.6. Налаштування ролей

Створимо роль адміністратора ідентифікації та керування доступом (IAM)

Створіть роль Identity Cloud Directory для підрядників.

CyberArk Identity використовує організації для делегування адміністративних завдань користувача певним особам. Уповноважені адміністратори можуть створювати користувачів, ролі та веб-програми та керувати ними. Лише глобальні адміністратори можуть створювати політики та керувати ними в CyberArk Identity.

Користувачі та уповноважені адміністратори можуть одночасно існувати лише в одній організації.

Окремих користувачів також можна додавати до організацій. Це може бути ручне оновлення або масове оновлення користувача.

Додавання окремого користувача

Усередині організації користувачів можна додавати за допомогою параметра «Учасники». Цей процес подібний до будь-якого іншого процесу, у якому ви додаєте користувачів і ролі.

Делегування керування веб-програмою

Уповноважені адміністратори можуть керувати веб-програмами, призначеними лише їхнім організаціям. Це зменшує обсяг керування, необхідне глобальному адміністратору, і дозволяє уповноваженому адміністратору надавати та керувати цими веб-програмами для своєї організації.

Тепер перейдемо до налаштування MFA. Щоб налаштувати MFA для всіх користувачів необхідно зробити наступні кроки:

Крок 1. Додайте новий набір правил

Увійдіть на портал адміністрування ідентифікаційної інформації .

Перейдіть до «Основні служби» > «Політики» та натисніть «Додати набір політик» , щоб створити нові правила.

Назвіть набір правил і виберіть Усі користувачі та пристрої .

Крок 2. Увімкніть елементи керування політикою автентифікації

Перейдіть до Політики автентифікації > Ідентифікація CyberArk .

Виберіть Так у розкривному списку Увімкнути елементи керування політикою автентифікації .

Крок 3. Створіть профіль автентифікації

В області «Правила автентифікації» виберіть « Додати новий профіль» із розкривного списку «Профіль за замовчуванням» .

Введіть унікальне ім’я для кожного профілю.

Виберіть механізм(и) автентифікації з кількох механізмів автентифікації або з одним механізмом автентифікації .

Розглянемо порядок налаштування Azure AD SSO для ідентифікації.

Для цього необхідно зробити наступні кроки.

1. Підтвердити свій основний домен на сторінці AAD, Extra ID.

2. Створити нову корпоративну програму

Приклад назви: CyberArk Identity Integration

Налаштуйте єдиний вхід на сторінці огляду програми CyberArk Identity Integration

Виберіть єдиний вхід, SAML.

3. З Identity - Settings - Users - External Identity Providers.

4. Розділ вхідних метаданих.

Введіть URL-адресу метаданих об'єднання додатків зі сторінки входу на основі SAML Entra ID, щось подібне до: https://login.microsoftonline.com/b7d75-07f-4323b1-34bb-c99221d23/federationmetadata/2007-06/federationmetadata.xml?appid=4bead5-ed-4a23a1-9034e7-e4725126c

5. Вихідні метадані.

Завантажте метадані з CyberArk Identity, а потім завантажте в програму CyberArk Identity Integration Entra ID

6. Після того, як ви натиснули «Зберегти», базова конфігурація SAML буде заповнена правильною інформацією, як це показано на рис.3.7.

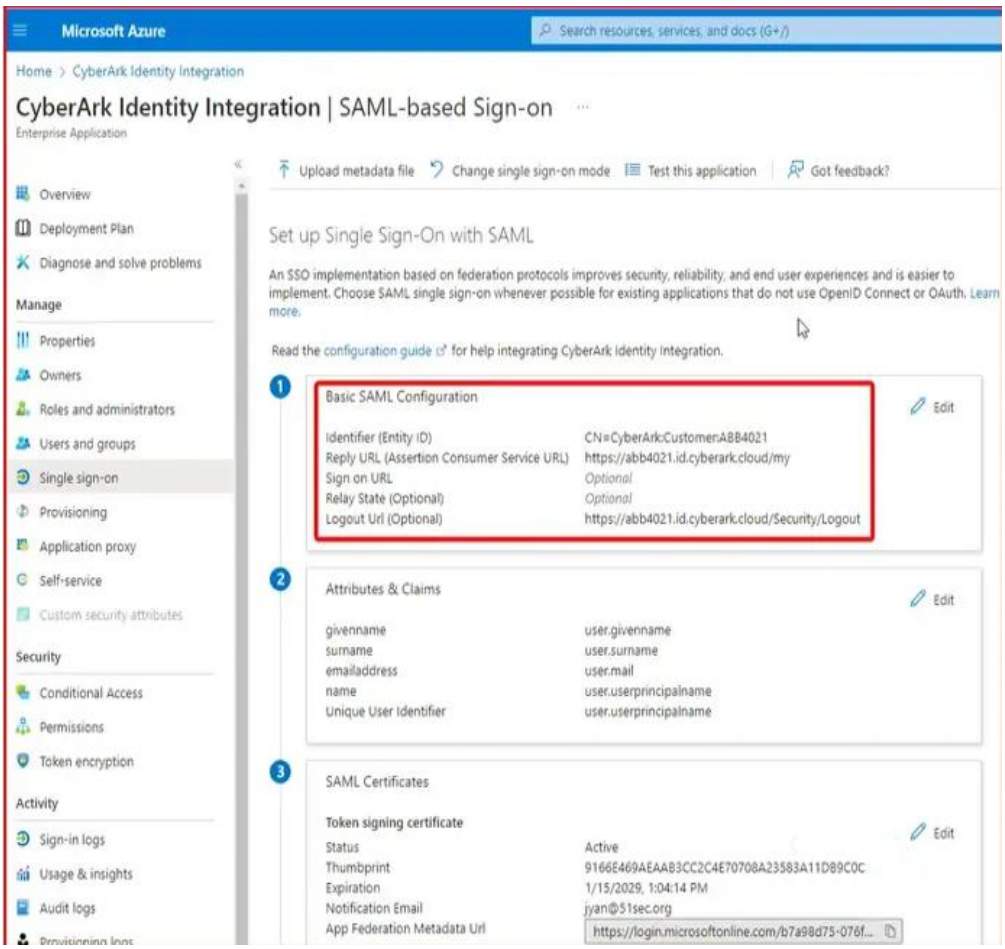
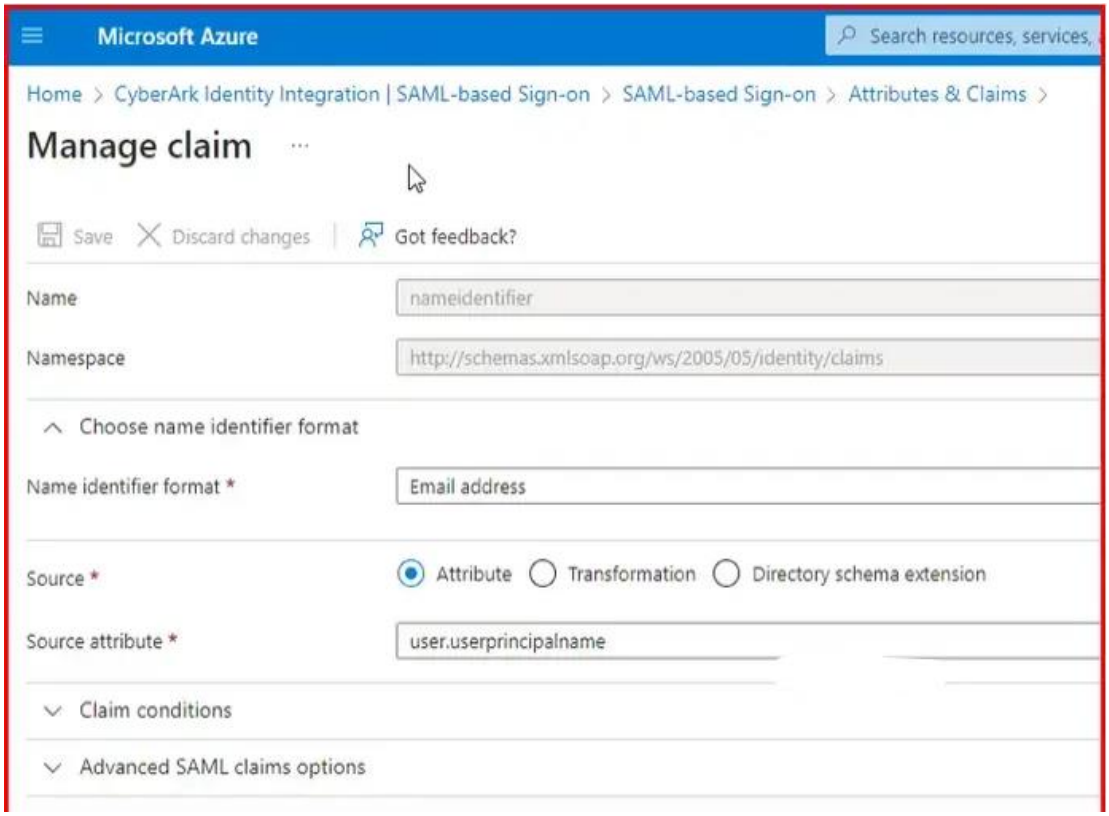


Рис.3.7. Базова конфігурація SAML

7. Додаємо назву атрибуту користувача як нові атрибути та претензію

(рис.3.8).



3.8. Назва атрибуту користувача

8. Призначте користувачів або групи до цієї програми CyberArk Identity Integration.

9. Додайте правила маршрутизації для зовнішнього постачальника посвідчень.

Отже, у практичній реалізації кваліфікаційної роботи показано порядок додавання засобів багатофакторної ідентифифікації MFA та підключення Azure AD SSO з використанням платформи CyberArk Identity, яка надає сучасні рішення для впровадження заходів захисту ідентифікації користувачів в інформаційній системі організації.

3.2. Розробка загальних рекомендацій щодо ідентифікації користувачів інформаційної системи

В даній кваліфікаційній роботі було досліджено засоби ідентифікацію користувачів інформаційних систем. Цей процес, хоч і може здаватися елементарним на перший погляд, насправді є дуже важливим для побудови та впровадження дієвих механізмів захисту. Правильно застосовані засоби ідентифікація користувачів є первинною умовою для реалізації ключових парадигм кібербезпеки та захисту інформації.

Коже фахівець повинен розуміти понятійний апарат щодо ідентифікації користувачів на кожному етапі. До сказаного належить:

Суб'єкт доступу (User/Principal)ю Будь-яка сутність (людина, процес, пристрій, сервіс), що взаємодіє з інформаційною системою та її ресурсами.

Ідентичність (Identity). Унікальний набір атрибутів та характеристик, що дозволяє відрізнити одного суб'єкта від іншого в межах системи.

Ідентифікація (Identification). Процес заявлення суб'єктом своєї ідентичності системі (наприклад, введення логіну).

Автентифікація (Authentication): Процес верифікації заявленої ідентичності (перевірка пароля, біометрії, токена тощо).

Авторизація (Authorization): Процес надання суб'єкту певних прав доступу до ресурсів на основі його підтвердженої ідентичності та визначених політик.

Роль (Role): Сукупність прав та привілеїв, що відповідає певній функції або посаді суб'єкта в контексті системи.

Процес ідентифікації є невід'ємною частиною базових принципів та моделей кібербезпеки в основу якої є модель AAA (Authentication, Authorization, Accounting): Ідентифікація є першим кроком, без якого неможлива ані автентифікація, ані авторизація, ані подальший облік дій (Accounting), що забезпечує невідмовність (Non-repudiation) та підзвітність.

Принцип Найменших Привілеїв (Principle of Least Privilege - PoLP): Надання суб'єкту лише мінімально необхідного набору прав для виконання його функцій

можливе тільки за умови точного визначення, хто є цим суб'єктом і які саме функції він виконує.

Розмежування Повноважень (Segregation of Duties - SoD). Запобігання конфлікту інтересів та шахрайству шляхом розподілу критичних завдань між різними користувачами/ролями вимагає чіткої ідентифікації цих ролей та їх функціональних обов'язків.

Управління ризиками. Неадекватна ідентифікація створює вразливості. Неідентифіковані або некоректно ідентифіковані суб'єкти (наприклад, "спільні" облікові записи, не деактивовані акаунти звільнених співробітників) збільшують поверхню атаки та ускладнюють атрибуцію шкідливих дій.

Конфіденційність, Цілісність, Доступність (CIA Triad): Контроль доступу, що базується на ідентифікації, є механізмом забезпечення всіх трьох складових тріади ЦРУ. Він обмежує доступ до конфіденційних даних, запобігає несанкціонованій модифікації (цілісність) і гарантує, що ресурси доступні лише авторизованим суб'єктам.

Підхід до ідентифікації користувачів інформаційної системи передбачає застосування комплексу методів, які повинні включати:

аналіз організаційно-штатної структури та функціональних обов'язків користувачів. посадових інструкцій для детермінації потенційних груп користувачів та їх функціональних потреб;

аналіз бізнес-процесів та робочих потоків (Workflow Analysis) для моделювання процесів, в яких задіяна інформаційна система, для виявлення всіх акторів (суб'єктів) та їх взаємодій на кожному етапі;

застосування якісних та кількісних методів збору даних від ключових стейкхолдерів (власників процесів, керівників підрозділів, потенційних користувачів) для уточнення ролей, завдань та вимог до доступу;

якщо інформаційна система замінює або інтегрується з існуючими, аналіз логів доступу, конфігурацій прав та списків користувачів може надати цінну та повну інформацію.

застосування рольових моделей (RBAC - Role-Based Access Control) спрощує адміністрування та забезпечує консистентність прав.

Необхідно звернути увагу на надання надлишкових привілеїв користуваям, які можуть призвести до загроз шляхом наступних дій:

неможливість відстежити дії конкретного співробітника (при використанні спільних акаунтів);

існування "облікових записів-привидів", які можуть бути скомпрометовані.

Проблеми з ідентифікацією, можуть призвести до ускладнення розслідування інцидентів безпеки, тому що буде неефективно працювати системи моніторингу та виявлення вторгнень (SIEM/IDS/IPS), які покладаються на коректну ідентифікацію суб'єктів.

Ну і звісно неправильні заходи та засоби ідентифікації користувачів приведуть до невідповідності регуляторним вимогам (напр., GDPR, HIPAA, PCI DSS), які вимагають чіткого контролю доступу та аудиту.

Одним з ефективних засобів для ідентифікації користувачів інформаційної системи організації є перехід моделей Нульової Довіри (Zero Trust), де ідентифікація суб'єкта та контекст доступу перевіряються постійно. Це пов’язано з розмитістю периметра безпеки організацій сьогодні.

Отже, процес ідентифікації користувачів є невід'ємною та критично важливою складовою теоретичного фундаменту та практичної реалізації кібербезпеки. Він безпосередньо впливає на ефективність ключових механізмів захисту, управління ризиками та відповідність нормативним вимогам. Глибоке розуміння застосування засобів ідентифікації та її зв'язку з основними принципами безпеки є обов'язковим для кваліфікованого фахівця з кібербезпеки.

ВИСНОВКИ

В результаті виконання кваліфікаційної роботи було отримано наступні результати:

Проаналізовано роль ідентифікації користувачів в інформаційній системі організації. У зв'язку з постійним збільшенням загроз, які пов'язані з конфіденційністю та несанкціонованим доступом питання доступу користувачів до ресурсів інформаційної системи організації є важливим питанням Для вирішення даної проблеми в роботі пропонується застосовувати комплексний підхід, тобто використання платформи, які надають послуги ідентифікації користувачів. В результаті проведеного порівняльного аналізу для ідентифікації користувачів було обрано рішення CyberArk Identity, яке пропонує різні засоби ідентифікації, такі як налаштування паролю, багатофакторна автентифікація, єдиний вхід до системи.

В роботі проаналізовано архітектуру рішення CyberArk Identity і досліджено можливості кожної з складової рішення. Аналаіз складових рішення дають цілісне уявлення щодо користувачів, їх ролі в ІС та засобів ідентифікації, які їм необхідно надавати.

В роботі надано варіант налаштування користувачів інформаційної системи організації, з використанням демо-версії CyberArk Identity. До варіанту налаштування ідентифікації користувачів створено основний алгоритм процесу налаштування багатофакторної автентифікації для користувачів, відповідно до виконаної ними ролі в інфраструктурі організації. Крім цього роботі представлено алгоритм налаштування Azure AD SSO для ідентифікації користувачів.

В результаті виконання роботи, було розроблено загальні рекомендації фахівцям з кібербезпеки, які необхідно враховувати при використанні засобів ідентифікації користувачів інформаційної системи організації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Що таке захист кінцевої точки. URL: *https://www.paloaltonetworks.com/cyberpedia/what-is-an-endpoint#:~:text=Endpoints%20are%20crucial%20in%20network,and%20the%20greater%20network%20infrastructure*.
2. Що таке кінцева точка? URL: https://www.cloudflare.com/learning/security/glossary/what-is-endpoint/ .
3. Повний посібник з рішень та найкращих практик захисту кінцевих точок. URL: https://www.bluevoyant.com/knowledge-center/complete-guide-to-endpoint-security-solutions-and-best-practices .
4. Що таке безпека кінцевих точок? URL: https://www.spiceworks.com/it-security/network-security/articles/what-is-endpoint-security/ .
5. Програмне забезпечення для керування кінцевими точками: моніторинг і керування пристроями. URL: https://www.ninjaone.com/endpoint-management/
6. Microsoft Intune—Керування кінцевою точкою | Microsoft Security. URL: https://www.microsoft.com/en-gb/security/business/microsoft-intune .
7. 6 найкращих випадків використання Microsoft Intune для ефективного керування кінцевими точками - ProServeIT. URL: https://www.proserveit.com/blog/microsoft-intune-endpoint-management-6-best-use-cases .
8. Керування мобільними пристроями (MDM) | Системний менеджер | Cisco Meraki. URL: https://meraki.cisco.com/products/systems-manager/ .
9. Що таке керування кінцевими точками? – Trellix. URL: https://www.trellix.com/security-awareness/endpoint/what-is-endpoint-security-management/ .
10. Endpoint Security (ENS) – Trellix. URL: https://www.trellix.com/products/endpoint-security/ .

11.Кращі практики менеджерів паролю. URL: https://community.cyberark.com/s/article/Workforce-Password-Manager-Best-Practices.

12.URL: https://docs.cyberark.com/identity/latest/en/content/getstarted/welcome.htm

13. URL: https://d1.awsstatic.com/Marketplace/solutions-center/downloads/AWSMP-CT-CyberArk-Datasheet.pdf.

14.Огляд порталу/ URL: https://docs.cyberark.com/identity-administration/latest/en/content/coreservices/core-overview.htm.

15.Процес налаштування ISPSS/ URL: https://docs.cyberark.com/ispss-deployment/latest/en/content/setup/setup_workflow_ispss.htm .

16.Користувачі та ролі URL: https://docs.cyberark.com/identity-administration/latest/en/content/ispss/ispss-add-system-users-and-roles.htm.

17. Aneta Poniszewska-Marand. Access control_models in heterogeneous information_systems From conception to exploitationComputer/ Science and Information Technology pp. 821–826 DOI:10.1109/IMCSIT.2008.4747337 .

18.Абдельфаттах, Д., Хассан, Х. А. та Омара, Ф. А. Новий алгоритм відображення ролей для покращення системи керування доступом, що забезпечує високий рівень співпраці. Паралельні бази даних Distrib 40 , 521–558 (2022). https://doi.org/10.1007/s10619-022-07407-9 .

19. Протокол RADIUS URL: https://datatracker.ietf.org/doc/html/rfc2865.

20. Налаштування CyberArk Identity для RADIUS URL: https://docs.cyberark.com/identity-compliance/latest/en/content/coreservices/authenticate/radiusconfig.htm .

21.Lightweight Directory Access Protocol (LDAP) URL: https://datatracker.ietf.org/doc/html/rfc4511

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)